ACOS 6.0.8
Command Line Interface Reference

December, 2025

© 2025 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Getting Started **78**

Introduction 78

Typographical Conventions 78

Accessing the CLI 79

CLI Quick Reference 80

Using the Help Command 80

Using the no Command 81

Using the Common Global Commands 81

Configuring and Viewing Command History 82

Viewing Context-Sensitive Help in the CLI 83

Editing Features and Shortcuts 85

Searching and Filtering CLI Output 89

Working with Regular Expressions 92

Adding Special Character in Strings 93

Tagging Objects 96

Enabling Baselining and Rate Calculation 97

Enable the Counters 97

View the Contents of the Counters 98

Session Access Levels 99

User EXEC Level 100

Privileged EXEC Level 100

Privileged EXEC Level - Config Mode 101

Global Configuration **102**

Configuration Commands 102

Privileged EXEC 102

axdebug 102

backup log 117

backup system 120

clear 122
clock 123
configure 123
diff 124
disable 125
exit 125
export 125
gen-server-persist-cookie 129
health-test 130
help 131
import 131
locale 149
no 150
ping 150
reboot 153
reload 155
repeat 156
shutdown 156
ssh 158
telnet 158
terminal 159
traceroute 162
write force 162
write memory 163
write terminal 165
EXEC 167
active-partition 167
enable 167
exit 168
help 168
no 168

show 169
Global 170
aam 170
access-list (standard) 170
access-list (extended) 175
accounting 183
acos-events 185
acos-events active-template 190
acos-events collector-group 191
acos-events log-server 193
acos-events message-id 194
acos-events message-selector 196
acos-events template 197
admin 198
admin cloud-cred 205
admin-lockout 208
admin-session clear 209
aflex 209
aflex-scripts start 210
arp 210
arp-timeout 211
audit 211
authentication console type 213
authentication enable 213
authentication login privilege-mode 214
authentication mode 214
authentication multiple-auth-reject 216
authentication type 216
authorization 218
automatic-update 220
backup store 230

backup-periodic 231
banner 234
bfd echo 235
bfd enable 235
bfd interval 235
block-abort 236
block-merge-end 237
block-merge-start 237
block-replace-end 238
block-replace-start 238
boot-block-fix 239
bootimage 239
bpdu-fwd-group 240
bridge-vlan-group 241
chassis-application-type 243
class-list 244
class-list (for Aho-Corasick) 245
class-list (for IP limiting) 246
class-list (for VIP-based DNS caching) 249
class-list (for many pools, non-LSN) 251
class-list (string) 253
class-list (string-case-insensitive) 253
configure sync 254
copy 256
delete 258
disable reset statistics 260
disable slb 261
disable-failsafe 261
disable-management 262
dnssec 265
do 268

domain-list 269
enable reset statistics 270
enable-core 271
enable-management 271
enable-password 276
end 277
environment temperature threshold 278
environment update-interval 279
erase 281
event 283
exit 283
fail-safe 284
fan-speed 286
file-system 287
glid 288
glm 293
hd-monitor enable 293
health global 294
health monitor 296
health source-nat 297
health-test 299
hostname 299
hsm template 300
hsm template template-name softHSM 300
hsm template template-name thalesHSM 301
icmp-rate-limit 302
icmpv6-rate-limit 303
import 304
import-periodic 322
import-periodic geo-location 329
import rpz 330

ip-list 333
l2-bfd 334
l3-vlan-fwd-disable 336
lacp system-priority 336
lacp-passthrough 337
ldap-server 337
link 339
lldp 340
locale 344
logging 345
mac-address 361
mac-age-time 362
maximum-paths 362
merge-mode-add 363
mirror-port 364
monitor 365
multi-config 367
multi-ctrl-cpu 367
netflow common max-packet-queue-time 371
netflow monitor 372
netflow template 378
netflow use-partition 382
no 383
ntp 384
object-group network 386
object-group service 389
offload-cpus 392
packet-handling 392
ping 393
poap 393
radius-server 393

raid 397
rba 397
resource-track 399
restore 401
route-map 402
router 408
router log file 409
router log log-buffer 410
run-hw-diag 410
running-config display 412
session-filter 412
sflow 414
smtp 417
snmp 419
so-counters 441
ssh-login-grace-time 443
sshd 444
syn-cookie 445
system 447
template 538
template ip-threat-action 540
tacacs-server host 541
tacacs-server monitor 545
techreport 546
terminal 548
tftp blksize 550
timezone 551
tx-congestion-ctrl 552
upgrade gui 552
upgrade hd 556
vcs 563

ve-stats 563
vlan 564
vlan-global enable-def-vlan-l2-forwarding 565
vlan-global l2-fwd-for-me-arp-ns 565
vlan-global l3-vlan-fwd-disable 566
web-service 566
write 571
Show Commands 571
show access-list 571
show acos-events messages 572
show active-partition 578
show admin 578
show aflex 584
show arp 585
show audit 586
show automatic-update 587
show axdebug capture 588
show axdebug config 589
show axdebug config-file 589
show axdebug file 590
show axdebug filter 592
show axdebug status 592
show backup 593
show bfd 594
show bootimage 602
show bpdu-fwd-group 602
show bridge-vlan-group 603
show bw-list 603
show class-list 605
show clns 606
show clock 608

show config 609
show config-block 609
show config-sync 609
show configure sync log 610
show context 612
show core 613
show core-slots 613
show counters-all slb hm-dplane 614
show counters acos-events statistics 616
show counters acos-events collector-group 619
show counters drop | error 619
show counters system ip-threat-list 620
show counters system session 622
show cpu 624
show debug 628
show disk 628
show dns cache 629
show dns-cache 646
show dns persistent-cache 646
show dns response-rate-limiting entries 647
show dns statistics 649
show dnssec 653
show dnssec dnskey 653
show dnssec ds 653
show dnssec statistics 654
show dnssec status 654
show dnssec template 654
show dumpthread 655
show environment 655
show errors 656
show event-action 660

show fail-safe 660
show file-system 663
show glid 667
show gui-image-list 668
show hardware 668
show health 669
show history 680
show icmp 681
show icmpv6 681
show interfaces 681
show interfaces brief 686
show interfaces media 689
show interfaces statistics 690
show interfaces transceiver 691
show ip 694
show ip anomaly-drop statistics 694
show ip bgp 699
show ip dns 700
show ip dns-cache 701
show ip fib | show ipv6 fib 701
show ip fragmentation 702
show ip helper-address 707
show ip interfaces | show ipv6 interfaces 712
show ip nat alg pptp 713
show ip nat interfaces | show ipv6 nat interfaces 715
show ip isis | show ipv6 isis 715
show ip nat pool | show ipv6 nat pool 715
show ip nat pool-group | show ipv6 nat pool-group 718
show ip nat range-list 718
show ip nat static-binding 719
show ip nat statistics 720

show ip nat template logging 720
show ip nat timeouts 721
show ip nat translations 721
show ip ospf | show ipv6 ospf 723
show ip prefix-list | show ipv6 prefix-list 723
show ip protocols | show ipv6 protocols 723
show ip rip | show ipv6 rip 723
show ip route | show ipv6 route 724
show ip stats | show ipv6 stats 725
show ip-list 726
show ipv6 ndisc 726
show ipv6 neighbor 728
show ipv6 traffic 729
show isis 730
show json-config 730
show json-config-detail 731
show json-config-with-default 732
show key-chain 733
show lacp 734
show lacp-passthrough 735
show license 736
show license-debug 736
show license-info 737
show lldp neighbor statistics 739
show lldp statistics 740
show locale 740
show local-log database 740
show local-uri-file 740
show log 741
show mac-address-table 742
show management 744

show memory 746
show mirror 749
show monitor 750
show netflow 750
show ntp 754
show pbslb 755
show pki 759
show poap 762
show process system 762
show radius-server 763
show reboot 763
show resource-accounting 764
show resource-tracked 768
show resource-tracked-by-user 769
show route-map 770
show router log file 770
show rpz 771
show run 773
show run visibility 775
show running-config 775
show session 778
show sflow 795
show shutdown 795
show smtp 795
show snmp engineID 796
show snmp oid 796
show snmp stats 800
show startup-config 801
show statistics 804
show store 806
show switch 806

show system app-performance 807
show system cpu-load-sharing 807
show system geo-location 809
show system ip-threat-list 813
show system inuse-rxtx-desc-info 814
show system inuse-rxtx-queue-info 815
show system job-offload statistics 815
show system link-monitor-polling-info 817
show system management-interface-mode 817
show system platform 818
show system path 819
show system port-list 821
show system radius server 823
show system radius table 825
show system rxtx-desc-info 826
show system rxtx-queue-info 827
show system resource-usage 827
show system shared-poll-mode 831
show system table-integrity 831
show system table-integrity statistics 832
show system tcp rate-limit-reset-unknown-conn 836
show system-ssl status 837
show tacacs-server 837
show techsupport 838
show terminal 841
show tftp 842
show trunk 842
show tsig 844
show version 845
show vlans 847
show vlan counter 848

show vlan counters 851
show vpn 852
clear dns cache 853
clear ip dns cache 859
clear system table-integrity 859

Application Delivery Partition 861

Configuration Commands 861
active-partition 861
application-type 862
partition 862
partition-admin 864
partition-group 868
service-partition 869
shared-vlan 871

Show Commands 877
show active-partition 877
show partition 877
show partition-config 879
show partition-group 880

ACOS Virtual Chassis System 881

Configuration Commands 881
device-context 881
vcs admin-session-connect 882
vcs database-distribution 884
vcs disable 884
vcs enable 885
vcs dead-interval 886
vcs dead-interval-mseconds 886
vcs debug 887
vcs device 888

vcs discovery-mode 890
vcs enable 892
vcs failure-retry-count 893
vcs floating-ip 894
vcs floating-ipv6 894
vcs force-wait-interval 895
vcs hold-preemption-interval 895
vcs multicast-ip 896
vcs multicast-ipv6 896
vcs multicast-port 897
vcs offload upgrade protocol <scp> 897
vcs reload 898
vcs ssl-enable 900
vcs time-interval 900
vcs time-interval-mseconds 901
vcs unicast-election 901
vcs vMaster-maintenance 903
vcs vmaster-take-over 904
Show Commands 905
show vcs debug 905
show vcs images 905
show vcs stat 907
show vcs summary 907
ACOS Virtual Router Redundant Protocol 911
Configuration Commands 911
migrate-vip 911
vrrp-a common 912
arp-retry 913
dead-timer 913
device-id 914

disable 914
disable-default-vrid 914
enable 915
forward-l4-packet-on-standby 915
get-ready-time 915
hello-interval 916
hop-limit 916
hostid-append-to-vrid 917
inline-mode 917
preemption-delay 918
restart-time 918
set-id 919
track-event-delay 919
ttl 920
vrrp-a fail-over-policy-template 920
vrrp-a force-self-standby 923
vrrp-a force-self-standby-persistent 924
vrrp-a interface 924
vrrp-a l2-inline-peer-ip 925
vrrp-a l3-inline-mode 926
vrrp-a ospf-inline 926
vrrp-a peer-group 927
vrrp-a preferred-session-sync-port ethernet 927
vrrp-a restart-port-list 928
vrrp-a vrid 929
vrrp-a vrid-lead 930
vrrp-a session-sync 931
vrrp-a vrid 931
blade-parameters 932
floating-ip 932
follow 933

preempt-mode 934
blade-parameters 935
fail-over-policy-template 935
priority 936
tracking-options 936
Show Commands 939
show vrrp-a 939
show vrrp-a all-partitions 944
show vrrp-a fail-over-policy-template 945
show vrrp-a hostid 946
show vrrp-a mac 946
show vrrp-a te-mac 947
show vrrp-a partition 947
show vrrp-a setid-monitor 948
show vrrp-a statistics 948
show vrrp-a vrid-lead 952
Scaleout 953
Configuration Commands 953
scaleout 953
scaleout apps enable 954
scaleout apps separate-v4-v6-traffic-map enable 954
scaleout active-user-group-assignment 954
scaleout distributed-forwarding fw 955
scaleout distributed-forwarding slb 956
scaleout user-group-assignment-template 957
cgnv6 scaleout nat-ip-hashing-scheme 962
cluster-devices 962
local-device 963
id 963
l2-redirect 963

priority 964
failure-domain 964
session-sync 965
start-delay 965
tracking-template 966
traffic-redirection 967
service-config 969
user-group-count 969
match scaleout 970
Show Commands 971
show cgnv6 scaleout 971
show scaleout 972
show scaleout failure-domain 978
show scaleout session-sync 979
show scaleout statistics 979
show scaleout traffic-map 988
show scaleout traffic-redirection 991
show scaleout user-group-assignment inside-user <IPv4 | IPv6> 992
show scaleout user-group-assignment template 993
Carrier-Grade NAT 996
Configuration Commands 996
Large Scale NAT 996
class-list (for LSN) 996
cgnv6 enable-port-batch-v1 997
cgnv6 ecmp 4-tuple-hash 998
cgnv6 global domain-list 998
cgnv6 logging 1000
cgnv6 lsn alg 1003
cgnv6 lsn alg sip rtp-stun-timeout 1004
cgnv6 lsn attempt-port-preservation 1005

cgnv6 lsn endpoint-independent-filtering 1005
cgnv6 lsn endpoint-independent-mapping 1006
cgnv6 lsn enhanced-user-tracking 1006
cgnv6 lsn hairpinning 1007
cgnv6 lsn half-close-timeout 1008
cgnv6 lsn health-check-gateway 1008
cgnv6 lsn icmp 1008
cgnv6 lsn inbound-refresh 1009
cgnv6 lsn inbound-refresh-full-cone 1009
cgnv6 lsn inside source class-list 1010
cgnv6 lsn ip-selection 1010
cgnv6 lsn logging default-template 1011
cgnv6 lsn logging partition 1012
cgnv6 lsn logging pool 1013
cgnv6 lsn port-batching 1013
cgnv6 lsn port-batching tcp-time-wait-interval 1013
cgnv6 lsn port-overloading 1014
cgnv6 lsn port-overloading allow-different-user 1014
cgnv6 lsn port-overloading unique 1015
cgnv6 lsn port-reservation 1015
cgnv6 lsn strictly-sticky-nat 1016
cgnv6 lsn stun-timeout 1016
cgnv6 lsn syn-timeout 1017
cgnv6 lsn tcp mss-clamp 1017
cgnv6 lsn tcp reset-on-error 1018
cgnv6 lsn-lid 1018
cgnv6 lsn-radius-profile 1023
cgnv6 lsn-rule-list 1024
cgnv6 nat icmp always-source-nat-errors 1035
cgnv6 nat icmp respond-to-ping 1035
cgnv6 nat icmpv6 respond-to-ping 1035

cgnv6 nat inside source static 1036
cgnv6 nat inside source static partition 1036
cgnv6 nat pool 1036
cgnv6 nat pool-group 1039
cgnv6 nat range-list 1040
cgnv6 nat exclude-port 1041
cgnv6 one-to-one mapping-timeout 1042
cgnv6 one-to-one pool 1042
cgnv6 one-to-one pool-group 1043
cgnv6 port-list 1044
cgnv6 resource-usage 1045
cgnv6 sctp rate-limit 1046
cgnv6 template http-alg 1046
cgnv6 translation 1049
ip-list 1050
netflow monitor 1052
session-filter 1056
DNS64 1057
cgnv6 nat pool 1057
cgnv6 nat pool-group 1057
cgnv6 nat64 prefix 1057
cgnv6 server 1058
cgnv6 service-group 1060
cgnv6 template dns 1060
cgnv6 dns64-virtualserver 1067
NAT64 1069
cgnv6 ecmp 4-tuple-hash 1069
class-list (for NAT64) 1069
glid (for NAT64 override) 1070
cgnv6 nat pool (for NAT64) 1071
cgnv6 nat pool-group (for NAT64) 1071

cgnv6 lsn-lid 1072
cgnv6 nat64 alg 1072
cgnv6 nat64 force-non-zero-ipv4-id 1074
cgnv6 nat64 fragmentation df-bit-transparency 1075
cgnv6 nat64 fragmentation inbound 1075
cgnv6 nat64 fragmentation inbound df-set 1076
cgnv6 nat64 fragmentation outbound 1076
cgnv6 nat64 icmp 1077
cgnv6 nat64 inside 1078
cgnv6 nat64 prefix 1078
cgnv6 nat64 tcp mss-clamp 1078
cgnv6 nat64 tcp reset-on-error 1079
cgnv6 nat64 user-quota-prefix-length 1079
cgnv6 template policy 1080
ip nat inside 1082
ip nat-global reset-idle-tcp-conn 1082
ip frag timeout 1082
ip frag max-reassembly-sessions 1083
Dual-Stack Lite Commands 1084
class-list (for DS-Lite) 1084
cgnv6 ds-lite alg 1085
cgnv6 ds-lite fragmentation inbound 1085
cgnv6 ds-lite fragmentation outbound 1086
cgnv6 ds-lite icmp 1087
cgnv6 ds-lite inside source class-list 1088
cgnv6 ds-lite ip-checksum-error 1088
cgnv6 ds-lite l4-checksum-error 1089
cgnv6 ds-lite port-reservation 1089
cgnv6 ds-lite tcp mss-clamp 1090
cgnv6 ds-lite tcp reset-on-error 1091
cgnv6 ds-lite user-quota-prefix-length 1091

Port Control Protocol Commands 1093
cgnv6 pcp default-template 1093
cgnv6 template pcp 1094
Logging Template Commands 1097
cgnv6 template logging 1097
cgnv6 server 1117
cgnv6 service-group 1119
Fixed-NAT Command 1120
cgnv6 ecmp 4-tuple-hash 1120
cgnv6 lsn alg 1120
cgnv6 fixed-nat create-port-mapping-file 1121
cgnv6 fixed-nat port-mapping-files-count 1122
cgnv6 fixed-nat inside 1122
Stateless NAT46 Commands 1126
cgnv6 nat46-stateless fragmentation inbound 1126
cgnv6 nat46-stateless fragmentation outbound 1126
cgnv6 nat46-stateless fragmentation outbound df-set 1127
cgnv6 nat46-stateless partition-prefix 1127
cgnv6 nat46-stateless prefix 1127
cgnv6 nat46-stateless static-dest-mapping 1128
cgnv6 nat46-stateless tcp mss-clamp 1130
Lightweight 4over6 Commands 1132
class-list (for lw4o6) 1132
cgnv6 lw-4o6 1132
cgnv6 lw-4o6 binding-table 1133
cgnv6 lw-4o6 binding-table-validate 1134
cgnv6 lw-4o6 fragmentation inbound 1134
cgnv6 lw-4o6 fragmentation outbound 1135
cgnv6 lw-4o6 hairpinning 1136
cgnv6 lw-4o6 health-check-gateway 1137
cgnv6 lw-4o6 icmp-inbound 1137

cgnv6 lw-4o6 inside-src-access-list 1138
cgnv6 lw-4o6 nat-prefix-list 1138
cgnv6 lw-4o6 no-forward-match 1138
cgnv6 lw-4o6 no-reverse-match 1139
cgnv6 lw-4o6 save-binding-table 1140
cgnv6 lw-4o6 use-binding-table 1140
MAP Commands 1141
cgnv6 map encapsulation domain 1141
cgnv6 map encapsulation fragmentation inbound 1142
cgnv6 map encapsulation fragmentation outbound 1143
cgnv6 map translation domain 1144
cgnv6 map translation fragmentation inbound 1146
cgnv6 map translation fragmentation inbound df-set 1147
cgnv6 map translation fragmentation outbound 1147
NPTv6 1148
cgnv6 nptv6 domain 1148
cgnv6 nptv6 common send-icmpv6-on-error disable 1148
6rd Commands 1150
cgnv6 sixrd domain 1150
cgnv6 sixrd fragmentation inbound 1151
cgnv6 sixrd fragmentation outbound 1152
cgnv6 sixrd fragmentation outbound df-set 1153
DDoS Mitigation 1154
acos-application-only 1154
cgnv6 ddos-protection 1154
cgnv6 ddos-protection disable-nat-ip-by-bgp zone 1154
cgnv6 ddos-protection logging 1155
cgnv6 ddos-protection max-hw-entries 1155
cgnv6 ddos-protection packets-per-second 1155
cgnv6 ddos-protection packets-per-second ip 1157
cgnv6 ddos-protection syn-cookie 1161

cgnv6 lsn-lid conn-rate-limit 1162
ip anomaly-drop 1163
ip anomaly-drop ipv6-ext-header 1164
Show Commands 1168
clear cgnv6 ddos-protection disabled-ip-by-bgp 1168
clear cgnv6 ddos-protection ip-entries 1168
clear cgnv6 ddos-protection l4-entries 1168
clear cgnv6 ddos-protection statistics 1168
show cgnv6 ddos-protection disabled-ip-by-bgp 1169
show cgnv6 ddos-protection ip-entries 1169
show cgnv6 ddos-protection l4-entries 1170
show cgnv6 ddos-protection statistics 1171
show cgnv6 dns64 statistics 1171
show cgnv6 ds-lite alg 1173
show cgnv6 ds-lite full-cone-sessions 1173
show cgnv6 ds-lite inside-user 1175
show cgnv6 ds-lite nat-address 1178
show cgnv6 ds-lite port-reservations 1180
show cgnv6 ds-lite statistics 1181
show cgnv6 ds-lite user-quota-sessions 1185
show cgnv6 fixed-nat alg 1188
show cgnv6 fixed-nat full-cone-sessions 1189
show cgnv6 fixed-nat histogram 1190
show cgnv6 fixed-nat inside-user 1190
show cgnv6 fixed-nat nat-address 1191
show cgnv6 fixed-nat port-mapping-files 1191
show cgnv6 fixed-nat statistics 1192
show cgnv6 l4 1197
show cgnv6 logging keywords 1198
show cgnv6 logging source-address 1202
show cgnv6 logging statistics 1202

show cgnv6 logging tcp-svr-status 1205
show cgnv6 lsn alg 1206
show cgnv6 lsn enhanced-user-tracking 1212
show cgnv6 lsn full-cone-sessions 1214
show cgnv6 lsn inside-user 1216
show cgnv6 lsn nat-address 1218
show cgnv6 lsn port-overloading config 1220
show cgnv6 lsn port-reservations 1220
show cgnv6 lsn statistics 1221
show cgnv6 lsn system-status 1228
show cgnv6 lsn user-quota-sessions 1230
show cgnv6 lsn-lid 1232
show cgnv6 lsn-rule-list 1232
show cgnv6 lw-4o6 binding-table 1234
show cgnv6 lw-4o6 binding-table-validation-log files 1235
show cgnv6 lw-4o6 statistics 1235
show cgnv6 map encapsulation domain 1238
show cgnv6 map encapsulation statistics 1239
show cgnv6 map translation domain 1239
show cgnv6 map translation statistics 1239
show cgnv6 nat pool 1240
show cgnv6 nat pool-group 1247
show cgnv6 nat range-list 1247
show cgnv6 nat static-binding 1248
show cgnv6 nat46-stateless statistics 1248
show cgnv6 nat64 alg 1250
show cgnv6 nat64 conversion 1251
1252
show cgnv6 nat64 enhanced-user-tracking 1252
show cgnv6 nat64 full-cone-sessions 1254
show cgnv6 nat64 inside-user 1256

show cgnv6 nat64 nat-address 1259
show cgnv6 nat64 prefixes 1261
show cgnv6 nat64 statistics 1261
show cgnv6 nat64 user-quota-sessions 1266
show cgnv6 nptv6 1269
show cgnv6 one-to-one mappings 1270
show cgnv6 one-to-one pool 1272
show cgnv6 one-to-one pool-group 1272
show cgnv6 one-to-one statistics 1272
show cgnv6 pcp statistics 1272
show cgnv6 resource-usage 1277
show cgnv6 sixrd statistics 1277
show cgnv6 template 1280
show counters cgnv6 fixed-nat hw-accelerate 1280
show counters cgnv6 fixed-nat per-instance 1282
show counters cgnv6 logging 1285
show counters cgnv6 lsn hw-accelerate 1288
show counters cgnv6 lsn per-instance 1290
show counters cgnv6 nat pool 1293
show counters cgnv6 nat64 hw-accelerate 1295
show ip anomaly-drop statistics 1297
show/clear lsn-alg esp 1299
show/clear nat64-alg esp 1299

Firewall 1301

Configuration Commands 1301
fw active-rule-set 1301
fw alg 1302
fw alg-processing 1304
fw allow-non-syn-session-create 1305
fw apply-changes 1306

fw clear-session-filter 1307
fw client class-list 1307
fw ddos-protection action 1309
fw ddos-protection dynamic-blacklist 1311
fw ddos-protection logging 1313
fw ddos-protection sampling-enable 1313
fw disable-application-category 1314
fw disable-application-metrics 1321
fw disable-application-protocol 1322
fw disable-ip-fw-sessions 1322
fw disable-undetermined-rule-logs 1323
fw dsr-mode-support 1323
fw extended-matching disable 1324
fw gtp apn-prefix-list 1325
fw gtp enable 1326
fw gtp insertion-mode apn-prefix-list 1326
fw gtp network-element-list-v4 1327
fw gtp network-element-list-v6 1328
fw gtp state-management 1329
fw hairpin next-hop-follow 1330
fw helper-sessions 1332
fw inbound-refresh 1333
fw inbound-refresh-full-cone 1333
fw listen-on-port-timeout 1334
fw local logging 1334
fw logging 1334
fw natip-ddos-protection 1336
fw permit-default-action 1336
fw respond-to-user-mac 1337
fw server 1338
fw service-group 1339

fw session-aging 1340
fw tcp mss-clamp 1344
fw tcp reset-on-error 1344
fw tcp-rst-close-immediate 1345
fw tcp syn-cookie 1346
fw tcp-window-check 1346
fw template logging 1347
fw urpf 1359
fw vrid 1360
object-group application 1361
rule-set 1361
remark 1362
rule 1363
rule-set rule action permit 1370
rule-set rule action-group permit 1372
rule-set rule action-group deny 1377
rule-set rule action-group reset 1378
sampling-enable 1379
application 1380
track-application 1380
session-statistic 1380
source 1381
dest 1382
system radius server 1383
template gtp 1388
template gtp-filter-list apn 1390
template gtp general-policy 1391
template gtp logging-policy 1392
template gtp msisdn-list 1393
template gtp rate-limit-policy 1394
template gtp-policy 1394

template limit-policy 1395
template limit-policy limit-pps 1401
template limit-policy limit-throughput 1403
template sctp 1405
traffic-control active-rule-set 1406
traffic-control rule-set 1407
remark 1407
rule 1408
zone 1413
Show Commands 1416
show automatic-update 1416
show counters fw alg 1416
show counters fw ddos-protection 1423
show counters fw global 1425
show counters fw gtp 1427
show counters fw hw-accelerate 1428
show counters fw logging 1430
show counters fw per-instance 1431
show counters fw rate-limit 1434
show counters fw server 1437
show counters fw service-group 1437
show counters fw tcp syn-cookie 1438
show counters fw tcp-window-check 1439
show counters rule-set 1439
show counters rule-set rule 1440
show counters sctp global 1442
show counters template gtp-policy 1443
show counters threat-intel threat-list 1446
show counters threat-intel webroot-global 1447
show fw application 1448
show fw ddos-protection entries 1450

show fw full-cone-sessions 1450
show fw limit-entry 1452
show fw logging-keywords 1453
show fw match 1455
show fw rate-limit 1456
show fw resource-usage 1460
show fw server 1462
show fw service-group 1463
show fw status 1465
show fw system-status 1467
show fw tcp syn-cookie statistics 1470
show fw top-k-rules 1471
show local-log database all/stats/file 1472
show rule-set 1474
show rule-set (application firewall) 1475
show sctp statistics 1482
show session application 1483
show session filter 1496
show session gtp 1503
show system radius server 1505
show system radius table 1506
show threat-intel database webroot 1508
show threat-intel ip-category 1509
show threat-intel log webroot 1510
show threat-intel hits webroot 1511
show traffic-control rule-set 1512
clear counters fw rate-limit 1513
clear counters threat-intel threat-list 1513
clear counters threat-intel webroot-global 1514
clear fw ddos 1514
clear fw ddos-protection 1514

clear fw full-cone-sessions 1515
clear fw tcp syn-cookie statistics 1515
clear fw top-k-rules 1515
clear sessions fw helper-sessions 1516
clear system radius server statistics 1517
clear system radius table 1517
clear tacacs-server statistics 1518
clear threat-intel hits webroot 1519

Next Generation Web Application Firewall 1520

Configuration Commands 1520
ng-waf 1520
license-manager ng-waf-module 1525
Show Commands 1526
clear ng-waf cache 1526
show ng-waf 1527
show ng-waf custom-page 1528
clear ng-waf custom-signals 1528
show ng-waf custom-signals 1528
show ng-waf status 1529
show ng-waf <virtual server> <port> 1532

Security Gateway 1540

Configuration Commands 1540
pki acme-cert 1540
account-email 1545
acme-client 1545
enroll 1546
log-level 1546
renew-before 1546
renew-every 1547
run-with-staging-server 1547

url 1548
pki acme-concurrent-process-count 1548
pki copy-cert 1549
pki copy-key 1550
pki cmp-cert 1551
cert-type 1551
cmp-ca 1552
cmp-cert 1552
log-level 1552
max-polltime 1553
recipient-dn 1553
renew-before 1553
renew-every 1554
secret 1554
subject-alternate-name 1555
pki create 1555
pki delete 1556
pki renew-self 1557
pki scep-cert 1558
dn 1558
enroll 1559
interval 1559
key-length 1559
log-level 1560
max-polltime 1560
method 1560
password 1561
renew-before 1561
renew-every 1561
subject-alternate-name 1562
san-domain 1562

system ipsec crypto-core 1562
system ipsec crypto-mem 1563
system ipsec fpga-decrypt 1563
system ipsec packet-round-robin 1563
vpn asymmetric-flow-support 1564
vpn extended-matching 1564
vpn fragment-after-encap 1564
vpn ike-logging-enable 1565
vpn ike-gateway 1565
auth-method 1565
configuration-payload 1567
dh-group 1567
dpd 1568
encryption 1569
interface-management 1571
ike-version 1571
key 1572
lifetime 1573
local-address 1573
local-cert 1573
local-id 1574
nat-traversal 1574
remote-address 1575
remote-ca-cert 1575
remote-id 1576
vrid 1576
radius-server 1577
vpn ike-acc-enable 1577
vpn ike-sa timeout 1578
vpn ike-stats-global 1578
vpn ipsec 1578

anti-replay-window 1579
bind 1580
crl 1580
dh-group 1580
dhcp-server 1581
disable 1582
disable-rekey 1582
domain 1582
enable 1582
encryption 1583
enroll 1585
force 1585
fragment-size 1585
ike-gateway 1586
lifebytes 1586
lifetime 1586
mode 1587
mtu 1587
proto 1588
sequence-number-disable 1588
speed 1588
traffic-selector 1588
up 1589
vpn ipsec-cipher-check 1590
vpn ipsec-group 1591
ipsec 1591
vpn jumbo-fragment 1592
vpn nat-traversal-flow-affinity 1592
vpn revocation 1593
ca 1593
ocsp 1593

vpn signature-authentication 1594
vpn stateful-mode 1594
vpn tcp-mss-adjust-disable 1595
Show Commands 1595
clear pki 1595
clear vpn crl 1596
clear vpn ike-sa 1596
clear vpn ike-stats 1596
clear vpn ike-stats-global 1597
clear vpn ipsec-group 1597
clear vpn ipsec-sa 1598
clear vpn log 1598
clear vpn ocsp 1598
debug monitor 1599
debug packet 1599
debug tunnel 1600
debug vpn level 1600
show counters-rate 1600
show counters vpn ike-gateway [NAME] 1602
show counters vpn ipsec [NAME] 1603
show hardware 1605
show vpn 1605
show vpn all-partitions 1606
show vpn partition <NAME> 1607
show vpn crl 1607
show vpn default 1608
show vpn ike-sa 1609
show vpn ike-sa-brief <NAME> 1611
show vpn ike-stats 1612
show vpn ike-stats-global 1613
show vpn ipsec-group 1615

show vpn ipsec-sa 1617
show vpn log 1620
show vpn ocsp 1620

Network Configuration 1622

Configuration Commands 1622
interface 1622
access-list 1625
bfd 1625
cpu-process 1628
dac-link-training-enable 1629
disable 1629
duplexity 1630
enable 1630
flow-control 1631
icmp-rate-limit 1631
icmpv6-rate-limit 1632
ip address 1634
ip address dhcp 1635
ip allow-promiscuous-vip 1636
ip cache-spoofing-port 1636
ip client 1637
ip control-apps-use-mgmt-port 1638
ip default-gateway 1639
ip helper-address 1640
ip igmp 1641
ip nat 1644
ip ospf 1645
ip rip authentication 1649
ip rip receive version 1650
ip rip receive-packet 1650

ip rip send version 1650
ip rip send-packet 1651
ip rip split-horizon 1651
ip router isis | ipv6 router isis 1651
ip server 1652
ip slb-partition-redirect 1652
ip stateful-firewall 1653
ip ttl-ignore 1653
ipv6 (on management interface) 1654
ipv6 access-list 1654
ipv6 address 1655
ipv6 enable 1656
ipv6 nat inside 1656
ipv6 nat outside 1656
ipv6 ndisc router-advertisement 1657
ipv6 ospf cost 1661
ipv6 ospf dead-interval 1662
ipv6 ospf hello-interval 1662
ipv6 ospf mtu-ignore 1662
ipv6 ospf neighbor 1663
ipv6 ospf network 1664
ipv6 ospf priority 1664
ipv6 ospf retransmit-interval 1665
ipv6 ospf transmit-delay 1665
ipv6 rip split-horizon 1665
ipv6 router isis 1666
ipv6 router ospf 1666
ipv6 router rip 1667
ipv6 stateful-firewall 1667
ipv6 ttl-ignore 1667
isis authentication 1668

isis bfd 1669
isis circuit-type 1669
isis csnp-interval 1670
isis hello 1670
isis hello-interval 1671
isis hello-interval-minimal 1671
isis hello-multiplier 1672
isis lsp-interval 1673
isis mesh-group 1673
isis metric 1674
isis network 1674
isis password 1675
isis priority 1675
isis restart-hello-interval 1676
isis retransmit-interval 1677
isis wide-metric 1677
l3-vlan-fwd-disable 1678
lldp enable 1678
lldp notification 1679
lldp tx-dot1-tlvs 1679
lldp tx-tlvs 1679
load-interval 1680
lw-4o6 1680
map-inside 1681
map outside 1681
media-type-copper 1681
monitor 1682
mtu 1683
name 1684
ports-threshold 1684
remove-vlan-tag 1685

snmp-server 1686
traffic-distribution-mode 1687
trunk-group 1688
virtual-wire 1689
ip 1690
ip access-list 1691
ip address 1695
ip anomaly-drop 1696
ip as-path 1697
ip community-list 1698
ip large-community-list 1699
ip default-gateway 1700
ip dmz 1700
ip dns 1701
ip extcommunity-list 1702
ip frag buff 1702
ip frag cpu-threshold 1703
ip frag max-packets-per-reassembly 1703
ip frag max-reassembly-sessions 1704
ip frag timeout 1704
ip icmp disable 1705
ip-list 1705
ip map-list 1705
ip mgmt-traffic 1706
ip nat alg dns 1707
ip nat alg pptp 1708
ip nat icmp 1708
ip nat inside source 1708
ip nat pool 1710
ip nat pool-group 1712
ip nat range-list 1713

ip nat template logging 1715
ip nat translation 1718
ip nat-global reset-idle-tcp-conn 1719
ip prefix-list 1720
ip reroute 1723
ip route 1724
ip tcp syn-cookie threshold 1725
ipv4-in-ipv6 frag 1726
ipv6 1726
ipv6 access-list 1726
ipv6 address 1730
ipv6 default-gateway 1731
ipv6 frag timeout 1731
ipv6 icmpv6 disable 1732
ipv6 nat icmpv6 respond-to-ping 1732
ipv6 nat inside source list 1733
ipv6 nat pool 1733
ipv6 nat pool-group 1734
ipv6 neighbor 1735
ipv6 ospf display route single-line 1736
ipv6 prefix-list sequence-number 1737
iv6p reroute 1738
ipv6 route 1739
ipv6-in-ipv4 frag 1741
router 1741
router rip 1742
router ipv6 rip 1755
router ospf 1765
router ipv6 ospf 1777
router isis 1795
router bgp 1816

router bgp 1855
bgp extended-asn-cap 1855
bgp nexthop-trigger 1857
trunk-stats 1857
virtual-wire 1857
virtual-wire <number> 1857
virtual-wire-ethernet-group 1859
virtual-wire-global 1859
virtual-wire-health-check 1860
virtual-wire-vlan-pair 1868
virtual-wire-vlan-pair-set 1870
vlan 1871
name 1872
router-interface 1873
shared-vlan 1873
tagged 1874
traffic-distribution-mode 1874
untagged 1876
untagged lif 1877
Show Commands 1878
clear [ip] bgp {* | AS-num} 1878
clear [ip] bgp external 1878
clear [ip] bgp ipv4 1879
clear [ip] bgp ipv4addr 1880
clear [ip] bgp ipv6 1880
clear [ip] bgp ipv6addr 1882
clear [ip] bgp peer-group 1882
clear [ip] bgp view 1883
clear ip rip route 1883
clear ipv6 rip route 1884
show [ip] bgp community 1884

show [ip] bgp community-list 1885
show [ip] bgp dampening 1885
show [ip] bgp filter-list 1886
show [ip] bgp inconsistent-as 1886
show [ip] bgp ipv4 {multicast | unicast} 1886
show [ip] bgp paths 1889
show [ip] bgp prefix-list 1889
show [ip] bgp quote-regexp 1889
show [ip] bgp regexp 1889
show [ip] bgp route-map 1890
show [ip] bgp summary 1890
show {ip | ipv6} ospf 1891
show {ip | ipv6} ospf interface 1892
show {ip | ipv6} ospf neighbor 1893
show {ip | ipv6} ospf route 1894
show {ip | ipv6} ospf virtual-links 1895
show bgp ipv4 neighbors 1896
show bgp ipv4 prefix-list 1897
show bgp ipv4 quote-regexp 1897
show bgp ipv4 summary 1898
show bgp ipv6 1898
show bgp ipv6addr 1901
show bgp nexthop-tracking 1901
show bgp nexthop-tree-details 1901
show ip bgp 1902
show ip bgp attribute-info 1903
show ip bgp cidr-only 1903
show ip bgp community-info 1903
show ip bgp ipv4addr 1903
show ip bgp scan 1904
show ip bgp view 1905

show ip isis [tag] route 1905
show ip ospf border-routers 1906
show ip ospf database 1907
show ip ospf redistributed 1909
show ip rip database 1911
show ip route acos 1912
show ipv6 isis [tag] route 1913
show ipv6 isis [tag] topology 1914
show ipv6 ospf database 1915
show ipv6 ospf topology 1917
show ipv6 rip database 1917
show isis [tag] database 1919
show isis [tag] topology 1920
show isis counter 1921
show isis interface 1923
show virtual-wire-global 1925
show virtual-wire-health-check 1926

Overlay Networks 1928

Configuration Commands 1928
debug packet 1928
interface lif 1930
overlay-mgmt-info 1930
overlay-tunnel vtep 1931
encap 1932
host 1933
local-ip-address 1934
remote-ip-address 1935
src-port-range 1938
vni 1939
overlay-tunnel options 1942

src-port-range 1945
Show Commands 1946
show interfaces brief 1946
show interfaces lif 1947
show overlay-tunnel 1948
show running-config overlay-mgmt-info 1950
show running-config overlay-tunnel 1951
show statistics interface 1952
show vlans 1953
Application Access Management 1954
Configuration Commands 1954
aam 1954
aam authentication 1955
aam authentication account 1955
aam authentication account kerberos-spn 1956
aam authentication account sampling-enable 1956
aam authentication global 1957
aam authentication jwt 1957
aam authentication log 1958
aam authentication log enable 1959
aam authentication log facility 1959
aam authentication logon 1960
aam authentication logon form-based 1960
aam authentication captcha 1964
aam authentication logon http-authenticate 1965
aam authentication portal 1967
aam authentication portal default-portal 1967
aam authentication relay 1975
aam authentication relay form-based 1975
aam authentication relay http-basic 1978

aam authentication relay kerberos 1979
aam authentication relay saml 1980
aam authentication relay ws-federation 1981
aam authentication saml 1982
aam authentication saml identity-provider 1982
aam authentication saml service-provider 1982
aam authentication server 1985
aam authentication server ldap 1986
aam authentication server ocsp 1988
aam authentication server radius 1989
aam authentication server windows 1991
aam authentication service-group 1992
aam authentication template 1993
aam authorization policy 1996
aam authentication oauth authorization-server 1999
aam authentication oauth client 2000
aam authentication relay oauth 2001
aam aaa-policy 2002
access-list 2002
action 2003
authentication-template 2003
authorize-policy 2004
captcha-authz-policy 2004
domain-name 2005
host 2005
match-encoded-uri 2006
port 2006
uri 2007
Show Commands 2008
clear aam authentication kcache 2008
clear aam authentication rdns 2008

clear aam authentication service-group 2008
clear aam authentication session 2008
clear aam authentication statistics 2009
clear aam authentication statistics jwt 2009
clear aam authorization jwt cache 2010
clear aam authentication saml idp status 2010
show aam aaa-policy 2011
show aam authentication 2011
show aam authentication account 2011
show aam authentication default-portal 2013
show aam authentication jwks 2013
show aam authentication klist 2014
show aam authentication logon 2016
show aam authentication logon form-based 2016
show aam authentication logon http-authenticate 2017
show aam authentication portal 2018
show aam authentication portal-image 2018
show aam authentication relay 2018
show aam authentication saml 2019
show aam authentication server 2019
show aam authentication service-group 2020
show aam authentication session 2021
show aam authentication session-attributes 2023
show aam authentication session-with-attributes 2023
show aam authentication statistics 2024
show aam authentication statistics captcha 2036
show aam authentication statistics jwt 2037
show aam authentication template 2037
show aam authorization jwt cache 2037
show aam authorization policy 2038

Global Server Load Balancing 2039
Configuration Commands 2039
delete geo-location 2039
gslb active-rdt 2040
gslb dns action 2041
gslb dns logging 2042
gslb geo-location 2043
gslb group 2044
gslb ip-list 2048
gslb policy 2049
active-rdt 2050
active-servers 2054
active-servers-enable 2055
admin-ip 2055
admin-ip-enable 2056
admin-preference 2056
alias-admin-preference 2057
auto-map 2057
bw-cost 2058
bw-cost-enable 2059
capacity 2059
connection-count-by-site 2060
connection-load 2061
dns action 2063
dns active-only 2063
dns addition-mx 2065
dns auto-map 2065
dns backup-alias 2066
dns backup-server 2067
dns cache 2067
dns cname-detect 2069

dns delegation 2070
dns external-ip 2070
dns external-soa 2071
dns geoloc-action 2072
dns geoloc-alias 2073
dns geoloc-policy 2074
dns hint 2075
dns ip-replace 2076
dns ipv6 mapping 2077
dns ipv6 mix 2079
dns ipv6 smart 2080
dns logging 2080
dns proxy block <query> 2082
dns proxy block <type> 2083
dns proxy block action 2085
dns selected-only 2086
dns server 2087
dns sticky 2090
dns sticky option 2092
dns ttl 2094
edns client-subnet geographic 2095
geo-location 2097
geo-location-match 2098
geographic 2100
health-check 2100
ip-list 2101
least-response 2101
metric-fail-break 2102
metric-force-check 2102
metric-order 2102
num-session 2103

num-session-enable 2105
round-robin 2105
weighted-alias 2106
weighted-ip 2107
weighted-ip-enable 2108
weighted-site 2108
weighted-site-enable 2109
dns server 2109
gslb protocol 2110
gslb protocol limit 2112
gslb secure-attributes 2113
gslb service-group 2115
gslb service-ip 2116
gslb service-matching-rules 2120
gslb site 2125
gslb sync-objects 2131
gslb system age-interval 2133
gslb system auto-map module 2133
gslb system auto-map ttl 2134
gslb system geo-location load 2134
gslb system ip-ttl 2135
gslb system wait 2136
gslb template csv 2136
gslb template snmp 2138
gslb zone 2141
import geo-location 2153
ip dns 2154
Show Commands 2155
show counters gslb dns 2155
show domain-list 2156
show gslb cache 2157

show gslb config 2159
show gslb fqdn 2161
show gslb geo-location 2162
show gslb group 2167
show gslb ip-list 2172
show gslb memory 2172
show gslb policy 2173
show gslb protocol 2174
show gslb rdt 2177
show gslb samples conn 2181
show gslb samples conn-load 2182
show gslb samples rdt 2184
show gslb service 2185
show gslb service-group 2188
show gslb service-ip 2188
show gslb service-port 2190
show gslb session 2191
show gslb site 2193
show gslb slb-device 2197
show gslb state 2198
show gslb statistics 2199
show gslb statistics secure 2201
show gslb zone 2201
clear gslb 2207

Server Load Balancing 2209

Configuration Commands 2209
health monitor 2209
default-state-up 2209
disable-after-down 2210
dsr-l2-strict 2210

header-insert 2211
health external 2211
interval 2213
method 2214
override-ipv4 2233
override-ipv6 2234
override-port 2234
passive 2234
proxy-header 2236
retry 2238
server-ssl 2238
ssl-ciphers 2240
ssl-ticket 2241
ssl-ticket lifetime 2241
ssl-version 2242
strictly-retry-on-server-error-response 2242
up-retry 2243
slb common 2244
aflex-table-entry-aging-interval 2244
aflex-table-entry-sync 2244
ecmp-hash 2246
low-latency 2246
service-group-on-no-dest-nat-vports 2247
buff-thresh 2248
cert-pinning 2248
compress-block-size 2250
conn-rate-limit src-ip 2251
ddos-protection 2252
ddos-protection logging 2253
ddos-protection packets-per-second 2253
disable-adaptive-resource-check 2254

disable-persist-scoring 2254
disable-server-auto-reselect 2255
dns-cache-age 2255
dns-cache-age-min-threshold 2257
dns-cache-aging-weight 2258
dns-cache-enable 2258
dns-cache-entry-size 2260
dns-cache-sync 2261
dns-cache-sync-entry-size 2261
dns-cache-sync-ttl-threshold 2262
dns-cache-ttl-adjustment-enable 2262
dns-cache-hitcount-enable 2262
dns-cookie-cache-policy 2263
dns-max-udp-size 2264
dns-negative-cache-enable 2264
dns-negative-cache-bypass-threshold 2265
dns-persistent-cache-enable 2266
dns-persistent-cache-hit-threshold 2266
dns-persistent-cache-ttl-threshold 2267
dns-response-rate-limiting 2267
dns-vip-stateless 2269
drop-icmp-to-vip-when-vip-down 2269
dsr-health-check-enable 2269
ecmp-hash 2270
enable-l7-req-acct 2270
extended-stats 2271
fast-path-disable 2272
gateway-health-check 2272
global-dns-cache 2273
graceful-shutdown 2276
honor-server-response-ttl 2277

hw-compression 2277
hw-syn-rr 2278
lb-method-hash 2279
l2l3-trunk-lb-disable 2280
max-buff-queued-per-conn 2281
max-http-header-count 2281
max-persistent-cache 2282
msl-time 2282
mss-table 2283
ng-waf 2284
no-auto-up-on-aflex 2289
odd-even-nat-enable 2290
pbslb-entry-age 2291
rate-limit-logging 2291
recursive-ns-cache 2293
reset-stale-session 2293
scale-out 2294
service-group-on-no-dest-nat-vports 2294
snat-gwy-for-l3 2295
snat-on-vip 2296
sort-res 2296
ssl-module 2298
ssli-sni-hash-enable 2300
ssli-silent-termination-enable 2304
stateless-sg-multi-binding 2305
stats-data-disable 2305
use-mss-tab 2306
slb forward-proxy 2306
slb resource-usage 2309
slb resource-usage threshold 2314
slb server 2314

support-http2 2317
alternate 2318
conn-limit 2318
conn-resume 2319
disable 2320
disable-with-health-check 2320
enable 2321
extended-stats 2321
external-ip 2321
health-check 2322
health-check-disable 2322
ipv6 2323
port 2323
slow-start 2329
spoofing-cache 2330
stats-data-disable 2330
stats-data-enable 2330
template server 2331
weight 2332
slb service-group 2332
backup-server-event-log 2334
extended-stats 2336
health-check 2336
health-check-disable 2337
member 2337
method 2341
min-active-member 2351
persist-scoring 2353
priority 2354
priority-affinity 2356
reset auto-switch 2357

reset-on-server-selection-fail 2357
sample-rsp-time 2357
stats-data-disable 2358
stats-data-enable 2358
strict-select 2358
template 2359
traffic-replication-type 2360
slb ssl 2362
slb ssl-cert-revoke sampling-enable 2362
slb ssl-expire-check email-address 2364
slb ssl-expire-check exception 2364
slb ssl-forward-proxy sampling-enable 2365
slb svm-source-nat pool 2366
slb template 2366
slb template cache 2367
accept-reload-req 2368
age 2369
default-policy-nocache 2369
disable-insert-age 2370
disable-insert-via 2370
max-cache-size 2370
max-content-size 2371
min-content-size 2372
packet-capture-template 2372
policy 2373
remove-cookies 2374
replacement-policy LFU 2374
template logging 2375
verify-host 2375
slb template cipher 2376
slb template connection-reuse 2378

slb template dblb 2379
slb template diameter 2380
slb template dns 2386
add-padding-to-client 2387
cache-hitcount-enable 2388
cache-record-serving-policy 2388
cache-ttl-adjustment-enable 2389
category-lookup 2389
category-lookup-bypass 2391
category-lookup-online-lookup 2392
class-list 2392
default-policy 2393
disable-dns-template 2393
disable-ra-cached-resp 2393
disable-rpz-attach-soa 2394
dns-cookie-cache-policy 2394
dns-log-enable 2395
dns64 2395
dnssec-service-group 2398
enable-cache-sharing 2399
insert-client-subnet 2399
malformed-query 2400
max-cache-entry-size 2401
max-cache-size 2401
max-query-length 2402
max-udp-size 2403
negative-dns-cache enable 2403
query-class-filter 2405
query-id-switch 2406
query-rate-monitoring 2407
query-type-filter 2408

recursive-dns-resolution 2409
redirect-to-tcp-port 2417
remove-aa-flag 2417
remove-edns-csubnet-to-server 2418
remove-padding-to-server 2418
response-rate-limiting 2418
rpz 2423
template 2424
tld-filter-log-enable 2424
tld-filter-white-list 2424
udp-retransmit 2425
slb template dns-logging 2426
slb template doh 2434
slb template dynamic-service 2439
slb template external-service 2441
slb template fix 2445
slb template ftp 2446
slb template http 2447
slb template http-policy 2469
slb template imap-pop3 2476
slb template link-block-as-down 2477
slb template link-cost 2478
slb template link-down-on-restart 2479
slb template link-probe 2480
destination hostname 2480
destination hostname target 2481
expected-status-code 2482
probe-interval 2483
probes-per-test 2483
rtt-method 2484
selection-rule 2485

test-interval 2485
url 2486
user-tag 2486
slb template logging 2487
slb template mqtt 2488
slb template monitor 2490
slb template persist cookie 2492
slb template persist destination-ip 2498
slb template persist source-ip 2502
slb template persist ssl-sid 2507
slb template policy 2508
acos-event-log 2511
action 2511
bw-list id 2513
bw-list name 2514
bw-list over-limit 2514
bw-list timeout 2515
bw-list use-destination-ip 2516
bw-rate-limit 2516
class-list 2517
conn-limit 2518
conn-rate-limit 2519
forward-policy 2519
forward-policy ssli-url-filtering 2543
forward-policy ssli-url-filtering-san 2544
geo-location full-domain-tree 2545
geo-location overlap 2546
geo-location share 2546
over-limit-action 2547
request-limit 2548
request-rate-limit 2548

response-code-rate-limit 2549
slb template port 2550
bw-rate-limit 2551
conn-limit 2552
conn-rate-limit 2552
dampening-flaps 2553
del-session-on-server-down 2554
dest-nat 2555
down-grace-period 2555
dscp 2556
dynamic-member-priority 2557
extended-stats 2558
health-check 2558
health-check-disable 2559
inband-health-check 2559
no-ssl 2561
request-rate-limit 2561
slow-start 2562
source-nat 2563
stats-data-disable 2564
stats-data-enable 2564
weight 2565
slb template quic 2566
slb template reqmod-icap 2568
allowed-http-methods 2569
disable-http-server-reset 2570
fail-close 2571
include-protocol-in-uri 2571
log-only-allowed-method 2571
min-payload-size 2572
preview 2572

service-group 2573
service-url 2574
template 2574
slb template respmod-icap 2575
disable-http-server-reset 2576
fail-close 2576
include-protocol-in-uri 2576
log-only-allowed-method 2577
min-payload-size 2577
preview 2578
service-group 2578
service-url 2579
template 2579
slb template server 2580
bw-rate-limit 2581
bw-rate-limit-acct 2582
conn-limit 2582
conn-rate-limit 2583
dns-query-interval 2584
dynamic-server-prefix 2585
extended-stats 2585
health-check 2585
health-check-disable 2586
l2-health-check-path 2586
log-selection-failure 2587
max-dynamic-server 2587
min-ttl-ratio 2588
slow-start 2588
spoofing-cache 2590
stats-data-disable 2590
stats-data-enable 2591

support-http2 2591
weight 2592
slb template sip (over TCP/TLS) 2592
alg-dest-nat 2593
alg-source-nat 2594
call-id-persist-disable 2594
client-keepalive 2594
client-request-header erase 2595
client-request-header insert 2595
client-response-header erase 2596
client-response-header insert 2597
dialog-aware 2598
exclude-translation 2598
failed-client-selection 2599
failed-server-selection 2599
insert-client-ip 2600
server-keep-alive 2600
server-request-header erase 2601
server-request-header insert 2601
server-response-header erase 2602
server-response-header insert 2603
server-selection-per-request 2604
smp-call-id-rtp-session 2604
timeout 2605
slb template sip (over UDP) 2606
alg-dest-nat 2606
alg-source-nat 2607
call-id-persist-disable 2607
client-request-header erase 2607
client-request-header insert 2608
client-response-header erase 2609

client-response-header insert 2609
dialog-aware 2610
exclude-translation 2611
insert-client-ip 2611
keep-server-ip-if-match-acl 2612
registrar service-group 2612
server-request-header erase 2612
server-request-header insert 2613
server-response-header erase 2614
server-response-header insert 2614
timeout 2615
slb template smpp 2616
client-enquire-link 2616
server-enquire-link 2617
server-selection-per-request 2617
user 2618
slb template smtp 2618
client-domain-switching 2620
command-disable 2621
server-domain 2622
service-ready-msg 2622
starttls 2623
slb template tcp 2623
del-session-on-server-down 2625
force-delete-timeout 2625
force-delete-timeout-100ms 2626
half-open-idle-timeout 2627
idle-timeout 2627
initial-window-size 2628
insert-client-ip 2628
lan-fast-ack 2629

proxy-header 2629
qos 2631
reset-follow-fin 2631
reset-fwd 2632
reset-rev 2632
slb template tcp-proxy 2633
proxy-header 2634
ack-aggressiveness 2635
backend-wscale 2636
del-session-on-server-down 2636
disable-abc 2637
disable-sack 2637
disable-tcp-timestamps 2638
disable-window-scale 2638
do-newsack 2638
dynamic-buffer-allocation 2639
early-retransmit 2639
fin-timeout 2640
force-delete-timeout 2641
force-delete-timeout-100ms 2641
half-close-idle-timeout 2642
half-open-idle-timeout 2642
idle-timeout 2643
init-cwnd 2644
initial-window-size 2644
insert-client-ip 2645
invalid-rate-limit 2646
keepalive-interval 2646
keepalive-probes 2648
limited_slowstart 2648
maxburst 2649

min-rto 2649
mss 2650
nagle 2650
naked-ack-on-handshake 2651
psh-flag-optimization 2651
qos 2652
reassembly-limit 2652
reassembly-timeout 2653
receive-buffer 2653
reno 2654
reset-fwd 2654
reset-rev 2654
retransmit-retries 2655
syn-retries 2656
timewait 2656
transmit-buffer 2657
slb template udp 2657
aging 2658
idle-timeout 2659
qos 2660
radius-lb-method 2661
re-select-if-server-down 2662
stateless-conn-timeout 2663
slb template virtual-port 2663
aflow 2665
allow-syn-otherflags 2666
allow-vip-to-rport-mapping 2666
conn-limit 2667
conn-rate-limit 2668
drop-unknown-conn 2669
dscp 2669

ignore-tcp-msl 2670
non-syn-initiation 2671
pkt-rate-limit 2671
reset-l7-on-failover 2673
reset-unknown-conn 2673
snat-msl 2674
snat-port-preserve 2674
slb template virtual-server 2675
conn-limit 2677
conn-rate-limit 2677
disable-when-all-ports-down 2678
disable-when-all-ports-down 2679
icmp-rate-limit 2679
icmpv6-rate-limit 2680
subnet-gratuitous-arp 2681
support-http2 2682
template server-ssl 2682
slb transparent-acl-template 2683
slb transparent-tcp-template 2684
slb virtual-server 2685
template client-ssl 2687
template server 2688
arp-disable 2689
description 2689
disable 2689
disable-when-all-ports-down 2690
disable-when-any-port-down 2690
enable 2691
extended-stats 2691
port 2691
redistribution-flagged 2695

stats-data-disable 2695
stats-data-enable 2696
template logging 2696
template policy 2696
template scaleout 2696
template virtual-server 2697
vrid 2697
slb virtual-server port 2699
aflex-table-entry-sync 2699
attack-detection 2699
aaa-policy 2700
access-list 2700
aflex 2702
alternate 2702
bucket-count 2703
clientip-sticky-nat 2703
conn-limit 2704
def-selection-if-pref-failed 2705
def-selection-if-pref-failed-disable 2707
disable 2707
enable 2707
extended-stats 2707
force-routing-mode 2708
gslb-enable 2708
ha-conn-mirror 2708
ipinip 2709
ip-map-list 2710
message-switching 2710
name 2710
no-auto-up-on-aflex 2710
no-dest-nat 2711

optimization-level 2712
rate-limit-pr-log 2714
redirect-fwd 2714
redirect-rev 2714
redirect-to-https 2715
reply-acme-challenge 2715
reset-on-server-selection-fail 2716
rtp-sip-call-id-match 2716
service-group 2717
skip-rev-hash 2718
snat-on-vip 2718
source-nat auto 2719
source-nat pool 2723
source-nat use-cgnv6 2723
stats-data-disable 2724
stats-data-enable 2724
support-http2 2724
syn-cookie 2725
template 2726
template virtual-port 2727
template quic 2728
use-default-if-no-server 2729
use-rcv-hop-for-resp 2729
when-server-selection-failed 2731
Show Commands 2732
show dns cache rate 2732
show hardware-accelerate slb statistics 2733
show hardware-accelerate statistics 2735
show hardware-accelerate status 2736
show hardware-forward slb statistics 2737
show hardware-forward statistics 2738

show hardware-forward status 2739
show run slb template 2739
show slb 2741
show slb aflow 2749
show slb attack-prevention 2751
show slb cache 2752
show slb common 2760
show slb compression 2761
show slb connection-reuse 2761
show slb conn-rate-limit 2763
show slb ddos-protection l4-entries 2765
show slb ddos-protection statistics 2766
show slb dns-custom-logging-keywords 2767
show slb diameter 2776
show slb fast-fix 2782
show slb fast-http-proxy 2783
show slb fix 2786
show slb forward-policy-source-port-translation-only-stats 2788
show slb ftp 2789
show slb ftp-proxy 2790
show slb generic-proxy 2790
show slb geo-location 2790
show slb http-proxy 2792
show slb http3 2805
show slb hw-compression 2816
show slb icap 2817
show slb icap-http 2819
show slb imap-proxy 2823
show slb l4 2826
show slb l7session 2840
show slb link-probe 2841

show slb mlb 2846
show slb mssql 2847
show slb mqtt 2849
show slb mysql 2851
show slb passthrough 2853
show slb persist 2854
show slb player-id-check-status 2857
show slb player-id-records-all 2857
show slb player-id-stats 2858
show slb pop3-proxy 2859
show slb quic 2860
show slb rate-limit-for-reset-unknown-conn 2878
show slb rate-limit-logging 2879
show slb resource-usage 2881
show slb server 2883
show slb service-group 2901
show slb sip 2908
show slb smpp 2910
show slb smtp 2917
show slb source-port-rate-limit 2921
show slb spdy-proxy 2922
show slb sshi 2924
show slb switch 2924
show slb syn-cookie 2932
show slb syn-cookie-buffer 2932
show slb tcp stack 2932
show slb template policy forward-policy-stats 2934
show slb virtual-server 2937
clear health https ssl-ticket 2979
clear slb unused-server-ports 2979
clear slb virtual-server 2981

Secure Socket Layer Insight **2984**
Configuration Commands 2984
slb template client-ssl 2984
auth-username 2986
auth-username-attribute 2987
authorization 2988
ca-cert 2989
certificate 2990
cipher 2991
client-certificate 2991
client-certificate-Request-CA 2992
close-notify 2993
crl 2994
dh-param 2995
direct-client-server-auth 2995
disable-sslv3 2995
early-data 2996
ec-name 2997
enable-ssli-ftp-alg 2999
enable-tls-alert-logging fatal 2999
forward-proxy-alt-sign cert 3000
forward-proxy-block-message 3001
forward-proxy-bypass ad-group-list 3001
forward-proxy-bypass case-insensitive 3002
forward-proxy-bypass central-cert-pin-list 3003
forward-proxy-bypass certificate-issuer 3004
forward-proxy-bypass certificate-san 3005
forward-proxy-bypass certificate-subject 3007
forward-proxy-bypass class-list 3009
forward-proxy-bypass client-auth 3010
forward-proxy-bypass client-ip-list 3012

forward-proxy-bypass contains 3013
forward-proxy-bypass ends-with 3014
forward-proxy-bypass equals 3015
forward-proxy-bypass exception-ad-group-list 3016
forward-proxy-bypass exception-class-list 3017
forward-proxy-bypass exception-client-ip-list 3017
forward-proxy-bypass exception-server-ip-list 3019
forward-proxy-bypass exception-user-name-list 3020
forward-proxy-bypass exception-web-category 3021
forward-proxy-bypass exception-web-reputation 3022
forward-proxy-bypass local-cert-pin-list 3023
forward-proxy-bypass require-web-category 3024
forward-proxy-bypass starts-with 3025
forward-proxy-bypass server-ip-list 3026
forward-proxy-bypass web-category 3027
forward-proxy-bypass web-reputation 3028
forward-proxy-ca-certificate 3029
forward-proxy-cache-persistence 3030
forward-proxy-cert-cache 3031
forward-proxy-cert-expiry 3032
forward-proxy-cert-ext 3032
forward-proxy-cert-not-ready-action 3033
forward-proxy-cert-revoke-action 3033
forward-proxy-cert-unknown-action 3034
forward-proxy-cert-validity 3036
forward-proxy-crl-disable 3036
forward-proxy-decrypted 3037
forward-proxy-enable 3037
forward-proxy-esni-action 3038
forward-proxy-failsafe-disable 3038
forward-proxy-inspect 3039

forward-proxy-inspect certificate-issuer 3040
forward-proxy-inspect certificate-san 3041
forward-proxy-inspect certificate-subject 3042
forward-proxy-log-disable 3042
forward-proxy-no-shared-cipher-action 3043
forward-proxy-no-sni-action 3043
forward-proxy-ocsp-disable 3044
forward-proxy-require-sni-cert-matched 3044
forward-proxy-selfsign-redir 3045
forward-proxy-source-nat 3045
forward-proxy-ssl-version 3046
forward-proxy-trusted-ca 3047
forward-proxy-verify-cert-fail-action 3048
handshake-logging-enable 3048
hsm-param 3049
ja3-enable 3049
ja3-insert-http-header 3049
ja3-reject-class-list 3050
ja3-reject-max-number-per-host 3051
ja4-enable 3052
ja4-insert-http-header 3053
ja4-reject-class-list 3053
ja4-reject-max-number-per-host 3054
local-logging 3055
non-ssl-bypass 3056
ocsp-stapling 3056
renegotiation-disable 3057
require-sni-cert-matched 3057
server-name 3058
server-name-auto-map 3059
server-name-regex 3060

server-name-bypass 3062
session-cache-size 3063
session-cache-timeout 3064
session-key-logging-enable 3064
session-ticket-disable 3064
session-ticket-lifetime 3065
ssl-false-start-disable 3065
ssli-inbound-enable 3066
ssli-logging 3067
sslv2-bypass 3068
template 3068
version 3069
slb template client-ssh 3070
forward-proxy-enable 3071
slb template server-ssl 3071
ca-cert 3074
certificate 3075
cipher 3075
close-notify 3076
crl 3077
dh-param 3077
early-data 3078
ec-name 3078
enable-ssli-ftp-alg 3079
enable-tls-alert-logging fatal 3079
forward-proxy-enable 3079
handshake-logging-enable 3080
ocsp-stapling 3080
renegotiation-disable 3080
server-certificate-error 3081
server-name 3082

session-cache-size 3082
session-cache-timeout 3082
session-key-logging-enable 3083
session-ticket-enable 3083
ssli-logging 3084
template cipher 3084
use-client-sni 3085
version 3085
slb template server-ssh 3086
forward-proxy-enable 3087
slb template ssli 3087
type 3088
debug ssl 3088
web-category 3090
Show Commands 3100
show slb ssl 3100
show slb ssl-cert-revoke-stats 3112
show slb ssl-counters 3115
show slb ssl-crl 3125
show slb ssl-cert-pinning-candidate-list 3130
show slb ssl-cert-pinning-candidate-list central-list 3132
show slb ssl-cert-pinning-candidate-list local-list 3134
show slb ssl-expire-check 3136
show slb ssl-forward-proxy-cert 3136
show slb ssl-forward-proxy-stats 3140
show slb ssl-ja3 3142
show slb ssl-ja4 3142
show slb ssl-ocsp cache 3143
show slb ssl-ocsp cache detail 3144
show web-category 3147
show web-reputation 3156

Cloud Services 3158
Configuration Commands 3158
cloud-services 3158
cloud-services cloud-provider 3159
cloud-services cloud-provider aws 3160
cloud-services cloud-provider aws log 3162
cloud-services cloud-provider aws metrics 3163
cloud-services cloud-provider aws multi-az-failover 3168
cloud-services cloud-provider azure 3171
cloud-services cloud-provider azure log 3172
cloud-services cloud-provider azure metrics 3174
cloud-services cloud-provider vmware 3181
cloud-services cloud-provider vmware log 3182
cloud-services cloud-provider vmware metrics 3184

Getting Started

The command-line interface (CLI) is an alternative to the web UI. This help provides a detailed list of commands along with valid syntax and examples necessary for configuring and managing the ACOS devices through CLI.

Introduction

The command-line interface (CLI) is an alternative to the web UI. This help provides a detailed list of global commands along with valid syntax and examples necessary for configuring and managing the ACOS devices through CLI.

The commands in each section are listed alphabetically. The following information is provided for each command:

- Command Name —The name of the command.
- Description—A brief description of the command.
- Syntax—The complete syntax of the command and the description of the command parameters.
- Mode - The mode in which the commands are available.
- Default - The default value set in the command, if any.
- Usage — Additional information to help you use the command, including: prerequisites, prohibitions, and workflows.
- Example—An example of how to use the command.
- Related Commands — The list of related commands, if any.

Typographical Conventions

The following typographical conventions are used for CLI command syntax or examples.

Fonts/Symbols	Meaning	Example
`text`	Indicates the CLI examples or the text that appears on the CLI.	!Section configuration: 77 bytes ! class-list my_class_list ac ends-with abc.com user-tag Security
bold	Indicates the CLI commands that you must enter or select, such as commands or command options.	**admin-session clear {all | session-id}**
Italics *with or without angle brackets <>*	Indicates the required parameter for which you must supply a value.	**[no] user-tag** *<name>* **[no] partition-group** *group-name*
Braces { }	Indicates the required choice.	**[no] vrrp-a preferred-session-sync-port {ethernet port-num [vlan** *vlan-id*] **trunk** *trunk-num <vlan vlan-id>*}
Square brackets [ ]	Indicates the optional commands or parameters available in the CLI command.	**partition-admin***partition-admin-username* **[password** *string***]**
Pipe character |	Indicates to choose one of the command options separated by the | symbol.	**show partition [all | available-id | port-ownership]**

Accessing the CLI

You can access the CLI through a console connection, an SSH session, or a Telnet session. Regardless of which connection method is used, access to the A10 Advanced Core Operating System (ACOS) CLI generally is referred to as an EXEC session or simply a CLI session.

NOTE: By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP, HTTPS, and SNMP access are enabled by default on the management interface only and disabled by default on all data interfaces.

CLI Quick Reference

Using the Help Command

Entering the **help** command (available at any command level) returns the CLI Quick Reference, as follows:

```
ACOS> help
CLI Quick Reference
===============
1. Online Help
Enter “?” at a command prompt to list the commands available at that CLI
level.
Enter "?" at any point within a command to list the available options.

Two types of help are provided:
1) When you are ready to enter a command option, type "?" to display each
possible option and its description.  For example: show ?
2) If you enter part of an option followed by "?", each command or option
that
matches the input is listed.  For example: show us?

2. Word Completion
The CLI supports command completion, so you do not need to enter the
entire
name of a command or option. As long as you enter enough characters of the
command or option name to avoid ambiguity with other commands or options,
the
CLI can complete the command or option.
After entering enough characters to avoid ambiguity, press "tab" to
auto-complete the command or option.

ACOS>
```

Using the no Command

Most configuration commands have **no** form. Typically, you use the no form to disable a feature or function. The command *without* the **no** keyword is used to re-enable a disabled feature or to enable a feature that is disabled by default; for example, if the terminal auto-size has been enabled previously. To disable terminal auto-size, use the **no terminal auto-size** form of the **terminal auto-size** command. To re-enable it, use the **terminal auto-size** form. This document describes the function of the **no** form of the command whenever a **no** form is available.

Using the Common Global Commands

Common commands that are available at all global configuration levels as listed below:

- backup log
- backup system
- clear
- do
- debug
- diff
- disable
- end
- exit
- export
- health-test
- help
- import
- no
- reboot

- reload
- repeat
- show
- write

Configuring and Viewing Command History

The CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. To use the command history feature, perform any of the tasks described in the following sections:

Setting the Command History Buffer Size

ACOS records 256 command lines in its history buffer, by default. To change the number of command lines that the system will record during the current terminal session, use the **terminal history** command.

From Privileged-EXEC mode, use the **terminal history** command to set the buffer size for the current session. For example, to set the buffer to 500, then verify the change with the show terminal command:

```
ACOS# terminal history size 500
ACOS# show terminal | sec history
History is enabled, history size is 500
ACOS#
```

Use the **no terminal history size** command to reset the buffer size for this session to the default value. For example:

```
ACOS# no terminal history size
ACOS# show terminal | sec history
History is enabled, history size is 256
ACOS#
```

If you use the **terminal history** command from Global configuration mode, you are making a more permanent change on the system; the buffer size will be the same for all configuration sessions, not just the current session.

Recalling Commands

To recall commands from the history buffer, use one of the commands or key combinations described in Recalling CLI Commands :

Table 1 : Recalling CLI Commands

Command or Key Combination	Description
Ctrl+P or Up Arrow key.	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. The arrow keys function only on ANSI-compatible terminals.
Ctrl+N or Down Arrow key.	Returns to more recent commands in the history buffer after recalling commands with Ctrl+P or the Up arrow key. Repeat the key sequence to recall successively more recent commands. The arrow keys function only on ANSI-compatible terminals.
ACOS> show history	While in EXEC mode, lists the most recent commands entered.

Viewing Context-Sensitive Help in the CLI

Enter a question mark (?) at the system prompt to display a list of available commands for each command mode. The context-sensitive help feature provides a list of the arguments and keywords available for any command.

To view help specific to a command name, a command mode, a keyword, or an argument, enter any of the commands summarized in Table 2:

Table 2 : CLI Help Commands

Prompt	Command	Purpose
ACOS> or ACOS# or (config)#	**Help**	Displays the CLI Quick Reference
	abbreviated-command-help?	Lists all commands beginning with abbreviation before the (?). If the abbreviation is not found, ACOS returns: % Unrecognized command. Invalid input detected at '^' marker.
	abbreviated-command-complete<Tab>	Completes a partial command name if unambiguous.
	?	Lists all valid commands available at the current level
	command ?	Lists the available syntax options (arguments and keywords) for the entered command.
	command keyword ?	Lists the next available syntax option for the command.

A space (or lack of space) before the question mark (**?**) is significant when using context-sensitive help. To determine which commands begin with a specific character sequence, type in those characters followed directly by the question mark; e.g. ACOS#**te?**. Do not include a space. This help form is called “word help” because it completes the word for you.

To list arguments or keywords, enter a question mark (?) in place of the argument or the keyword. Include a space before the (?); e.g. ACOS# **terminal ?**. This form of help is called “command syntax help” because it shows you which keywords or arguments are available based on the command, keywords, and arguments that you already entered.

Users can abbreviate commands and keywords to the minimum number of characters that constitute a unique abbreviation. For example, you can abbreviate the **config terminal** command to **conf t**. If the abbreviated form of the command is unique, then ACOS accepts the abbreviated form and executes the command.

Context Sensitive Help Examples

The following example illustrates how the context-sensitive help feature enables you to create an access list from configuration mode.

Enter the letters **co** at the system prompt followed by a question mark (**?**). Do not leave a space between the last letter and the question mark. The system provides the commands that begin with co.

```
ACOS# co?
  configure  Entering config mode
ACOS# co
```

Enter the **configure** command followed by a space and a question mark to list the keywords for the command and a brief explanation:

```
ACOS# configure ?
  terminal  Config from the terminal
  <cr>
ACOS# configure
```

The <cr> symbol ("cr" stands for carriage return) appears in the list to indicate that one of your options is to press the Return or Enter key to execute the command, without adding any additional keywords.

In this example, the output indicates that your only option for the **configure** command is **configure terminal** (configure manually from the terminal connection).

Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the CLI.

Positioning the Cursor on the Command Line

The table below lists key combinations used to position the cursor on the command line for making corrections or changes. The Control key (ctrl) must be pressed simultaneously with the associated letter key. The Escape key (esc) must be pressed first, followed by its associated letter key. The letters are not case-sensitive. Many letters used for CLI navigation and editing were chosen to simplify remembering their functions. In Table 3, characters bolded in the Function Summary column indicate the relation between the letter used and the function.

Table 3 : Position the Cursor in the CLI

Keystrokes	Function Summary	Function Details
Left Arrow or ctrl+B	Back character	Moves the cursor left one character. When entering a command that extends beyond a single line, press the Left Arrow or Ctrl+B keys repeatedly to move back toward the system prompt to verify the beginning of the command entry, or you can also press Ctrl+A.
Right Arrow or ctrl+F	Forward character	Moves the cursor right one character.
ctrl+A	Beginning of line	Moves the cursor to the very beginning of the command line.
ctrl+E	End of line	Moves the cursor to the very end of the line.

Completing a Partial Command Name

If you do not remember a full command name, or just to reduce the amount of typing you have to do, enter the first few letters of a command, then press tab. The CLI parser then completes the command if the string entered is unique to the command mode. If the keyboard has no tab key, you can also press ctrl+I.

The CLI will recognize a command once you enter enough text to make the command unique. For example, if you enter **conf** while in the privileged EXEC mode, the CLI will associate your entry with the config command, because only the config command begins with conf.

In the next example, the CLI recognizes the unique string **conf** for privileged EXEC mode of config after pressing the tab key:

```
ACOS# conf<tab>
ACOS# configure
```

When using the command completion feature, the CLI displays the full command name. Commands are not executed until the Enter key is pressed. This way you can modify the command if the derived command is not what you expected from the abbreviation. Entering a string of characters that indicate more than one possible command (for example, **te**) results in the following response from the CLI:

```
ACOS# te
% Ambiguous command
ACOS#
```

If the CLI can not complete the command, enter a question mark (?) to obtain a list of commands that begin with the character set entered. Do not leave a space between the last letter you enter and the question mark (?).

In the example above, **te** is ambiguous. It is the beginning of both the telnet and terminal commands, as shown in the following example:

```
ACOS# te?
  telnet    Open a telnet connection
  terminal  Set Terminal Parameters, only for current terminal
ACOS# te
```

The letters entered before the question mark (**te**) are reprinted to the screen to allow continuation of command entry from where you left off.

Deleting Command Entries

If you make a mistake or change your mind, use the keys or key combinations in Deleting CLI Entries to delete command entries:

Table 4 : Deleting CLI Entries

Keystrokes	Purpose
backspace	The character immediately left of the cursor is deleted.
delete or **ctrl+D**	The character that the cursor is currently on is deleted.
ctrl+K	All characters from the cursor to the end of the command line are deleted.
ctrl+U or **ctrl+X**	All characters from the cursor to the beginning of the command line are deleted.
ctrl+W	The word to the left of the cursor is deleted.

Editing Command Lines that Wrap

The CLI provides a wrap-around feature for commands extending beyond a single line on the display.

When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, press **ctrl+B** or the left arrow key repeatedly until you scroll back to the command entry, or press **ctrl+A** to return directly to the beginning of the line.

The ACOS software assumes you have a terminal screen that is 80 columns wide. If you have a different screen-width, use the **terminal width** EXEC command to set the width of the terminal.

Use line wrapping in conjunction with the command history feature for Recalling Commands and modifying previous complex command entries.

Continuing Output at the --MORE-- Prompt

When working with the CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many **?**, **show**, or **more** commands, the output is paused and a **--MORE--** prompt is displayed at the bottom of the screen.

To proceed, press the Enter key to scroll down one line, or press the spacebar to display the next full screen of output.

Redisplaying the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command line entry. To redisplay the current command line (refresh the screen), use either **ctrl+L** or **ctrl+R**.

Editing Pre-Configured Items

You can display a list of some items that have been configured on the ACOS device (for example, SLB objects, partitions, object-groups) by entering the partial command, followed by the '?' character. Previous releases required you to know the exact name of the real server or other items you wanted to modify, but this feature enables you to display the items that are already configured without having to remember the exact name.

For example, the following SLB items can be viewed in this manner:

- **slb server**
- **slb service-group**

- **slb virtual-server**
- **member** (at service-group configuration level)
- **service-group** (at virtual-port configuration level)

The following example displays the names of real servers that are already configured on the ACOS device. All options displayed in the output except “NAME” are real servers.

```
ACOS(config)# slb server ?
  realserver1
  realserver2
  rs1
  rs2
  rs3
NAME<length:1-127>  Server Name
ACOS(config)# slb server
```

You can further refine the list that appears by entering part of the name. For example:

```
ACOS(config)# slb server rs?
  rs1
  rs2
  rs3
  NAME<length:1-127>  Server Name
ACOS2(config)# slb server a
```

In the same manner that commands can be auto-completed by partially entering the command name and pressing <TAB>, the ACOS device supports the ability to auto-complete the names of configured items. For example:

```
ACOS(config)# slb server re<TAB>
ACOS(config)# slb server realserver
```

Searching and Filtering CLI Output

This section contains the following topics:

Common Output Filters

The CLI permits searching through large amounts of command output by filtering

the output to exclude information that you do not need. The **show** command supports the output filtering options described in show Command Output Filters :

Table 5 : show Command Output Filters

Filter	Description
begin *string*	Begins the output with the line containing the specified string.
include *string*	Displays only the output lines that contain the specified string.
exclude *string*	Displays only the output lines that *do not* contain the specified string.
section *string*	Displays only the lines for the specified section (for example, “slb server”, “virtual-server”, or “logging”). To display all server-related configuration lines, you can enter “server”.

Advanced Output Filters

Some **show** commands (for example, **show log**) provide additional output filtering options described in show log Command Output Additional Filters . These options are a subset of the standard sort commands available on UNIX operating systems.

Table 6 : show log Command Output Additional Filters

Filter	Description
grep [**invert-match**] *string*	Display only those lines matching the specified **grep** expression. **NOTE:** If the **grep** expression matches the same letters as “invert-match” the command will fail since the CLI will not be able to distinguish between the **invert-match** option and a desired **grep** patten. To work around this issue, enclose the desired **grep** expression in quotation marks. For example, the following command would be invalid: **show log | grep in** However, the following would return the desired result:

Table 6 : show log Command Output Additional Filters

Filter	Description
	show log | grep "in"
awk [**fs***separator*] **print** *expression*	Displays only the fields matching the specified **awk** expression. **NOTE:** When specifying multiple expressions, use quotations marks if you need to have spaces. For example, the following expressions are both valid; the first one prints two fields with no space, the second encloses the space within quotation marks: **show log | awk fs : print $1,$2** **show log | awk fs : print "$1, $2"**
cut [**delimiter***char*] **fields***field*	Do not show the output matching the specified **cut** expression.
sort [**numeric-sort**] [**reverse**] [**unique**]	Sort the lines in the output based on the specified **sort** expression.
uniq [**skip-chars***num*] [**skip-fields** *num*] [**count**] [**repeated**]	Show only unique lines in the output as defined by the specified options.

Examples of Filtering Output

Use the pipe " | " character as a delimiter between the **show** command and the display filter.

Example 1—Using Working with Regular Expressions to Match a String

You can use regular expressions in the filter string, as shown in the following example:

```
ACOS(config)# show arp | include 192.168.1.3*
```

```
192.168.1.3         001d.4608.1e40        Dynamic      ethernet4
192.168.1.33        0019.d165.c2ab        Dynamic      ethernet4
```

The output filter displays only the ARP entries that contain IP addresses that match “192.168.1.3” and any value following “3”. The asterisk (*) matches on any pattern following the “3”.

Example 2—Viewing a Specific Section of the Configuration

The following example displays the startup-config lines for “logging”:

```
ACOS(config)# show startup-config | section logging
logging console error
logging buffered debugging
logging monitor debugging
logging buffered 30000
logging facility local0
```

Example 3—Viewing Unique Output Strings

The following example shows how to use the advanced options to string multiple filters together so that unique error log messages are displayed:

```
AX5100(config)# show log | grep Error | sort | uniq
Apr 03 2015 01:55:42 Error   [SYSTEM]:The user, admin, from the remote
host, 172.17.1.169:52130, failed in the CLI authentication.
Apr 06 2015 21:48:45 Error   [SYSTEM]:The user, admin, from the remote
host, 172.17.1.169:51582, failed in the CLI authentication.
Apr 08 2016 08:52:36 Error   [SYSTEM]:The user, admin, from the remote
host, 172.17.0.224:62585, failed in the CLI authentication.
Apr 08 2016 19:58:13 Error   [CLI]:Failed to register routing module
commands
Apr 08 2016 19:58:13 Error   [CLI]:Unrecognized command: "ospf" in
module if
...
```

Working with Regular Expressions

Regular expressions are patterns (e.g. a phrase, number, or more complex pattern) used by the CLI string search feature to match against the **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching

requirements. A simple regular expression can be an entry like Serial, misses, or 138. Complex regular expressions can be an entry like 00210..., (is), or [Oo]utput.

A regular expression can be a single-character pattern or a multiple-character pattern. This means that a regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. The pattern in the command output is referred to as a *string*. This section describes creating single-character patterns.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A–Z, a–z) or digit (0–9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. Table 7 list the keyboard characters that have special meaning.

Table 7 : Single-Character Regular Expression Patterns

Character	Meaning
.	Matches any single character, including white space
*	Matches 0 or more sequences of the pattern
+	Matches 1 or more sequences of the pattern
?	Matches 0 or 1 occurrences of the pattern
^	Matches the beginning of the string
$	Matches the end of the string
_ (underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis (( ), right parenthesis ( )), the beginning of the string, the end of the string, or space.

Adding Special Character in Strings

Special characters are supported in password strings and various other strings. To use special characters in a string, enclose the entire string in double quotation

marks.

This section contains the following topics:

Special Character Support in Passwords and Strings

The following subsections list the special characters supported for each type of password you can enter in the CLI.

Table 8 : Special Characters in Passwords and Strings

Password Type	Special Character Support
Admin and Enable password	Admin and enable passwords can contain any ASCII characters in the following ranges: 0x20-0x7e and 0x80-0xFF.
ACOS device hostname RADIUS shared secret SNMPv3 user authentication passwords	Strings for these items can contain any of the following ASCII characters `a-z A-Z 0-9 - . ( )`
RADIUS shared secrets	The device hostname can contain any of the following ASCII characters `a-z A-Z 0-9 - . ( )`
MD5 passwords for OSPF or BGP	MD5 passwords can be up to 16 characters long. A password string can contain any ASCII characters in the range 0x20-0x7e. The password string can not begin with a blank space, and can not contain any of the following special characters: `' " < > & \ / ?`
Passwords used for file import or export	All of the characters in the following range are supported: 0x20-0x7E.
Passwords user for server	Most of the characters in the following range are supported: 0x20-0x7E.

Table 8 : Special Characters in Passwords and Strings

Password Type	Special Character Support
access in health monitors	The following characters are not supported: " < > & \ / ?
SSL certificate passwords	Most of the characters in the following ranges are supported: 0x20-0x7E and 0x80-0xFF.
SMTP passwords	The following characters are not supported: ' " < > & \ / ?

How To Enter Special Characters in the Password String

You can use an opening single-or double-quotation mark without an ending one. In this case, `'"` becomes `"`, and `"'` becomes `'`.

Escape sequences are required for a few of the special characters:

- `"` – To use a double-quotation mark in a string, enter the following:`\"`
- `?` – To use a question mark in a string, enter the following sequence:`\077`
- `\` – To use a back slash in a string, enter another back slash in front of it:`\\`

For example, to use the string a"b?c\d, enter the following: `"a\"b\077c\\d"`

The `\` character will be interpreted as the start of an escape sequence only if it is enclosed in double quotation marks. (The ending double quotation mark can be omitted.) If the following characters do not qualify as an escape sequence, they are taken verbatim; for example, `\` is taken as `\`, `"\x41"` is taken as **A** (hexadecimal escape), `"\101"` is taken as **A** (octal escape), and `"\10"` is taken as `\10`.

NOTE: To use a double-quotation mark as the entire string, `"\""`. If you enter `\"`, the result is `\`. Using a single character as a password is not recommended. It is recommended not to use i18n characters. The character encoding used on the terminal during password change might differ from the character encoding on the terminal used during login.

Tagging Objects

Certain objects created in the CLI can be tagged by using the **user-tag** command. These tags can then be searched by using the aXAPI. For more information, see "Filters" page of the *aXAPI Reference*.

NOTE: Do not enter the value "Security" for the custom tag from the CLI; this is a reserved keyword. Doing so can interfere with the proper display of SSLi configurations performed in the GUI.

Tagging objects is useful to help differentiate objects that can be used for multiple feature areas, like real servers, virtual servers, service groups, or templates. Consider the following example, where multiple real servers are created for load balancing. By tagging each server, the **show running-config** output can help you identify which servers are used for FTP load balancing (labeled with "FTP") and which ones are used for HTTP load balancing (labeled with "HTTP):

```
ACOS(config)# slb server ftp1 192.168.1.1
ACOS(config-real server)# user-tag FTP-1
ACOS(config-real server)# exit
ACOS(config)# slb server ftp1 192.168.2.2
ACOS(config-real server)# user-tag FTP-2
ACOS(config-real server)# exit
ACOS(config)# slb server http1 192.168.10.10
ACOS(config-real server)# user-tag HTTP-1
ACOS(config-real server)# exit
ACOS(config)# slb server http2 192.168.20.20
ACOS(config-real server)# user-tag HTTP-2
ACOS(config-real server)# show running-config | sec slb server
slb server ftp1 192.168.1.1
  user-tag FTP-1
slb server ftp2 192.168.2.2
  user-tag FTP-2
slb server http1 192.168.10.10
  user-tag HTTP-1
slb server http2 192.168.20.20
  user-tag HTTP-2
```

At a later point in time, suppose server “ftp1” needs to be re-purposed; rather than renaming the server and all of the corresponding configuration that might also have “FTP” in their object names, you can update the user tag to indicate the actual purpose of the server while leaving the existing configuration intact.

Tags can be 1-127 characters in length.

Enabling Baselining and Rate Calculation

The **sampling-enable** command enhances the information that can be viewed for statistical counters in the system. By using this command in conjunction with **show counters-baselining** and **show counters-rate**, you can obtain additional counter statistics to help you baseline specific portions of your configuration to troubleshoot or improve performance.

To enable this:

- Enable the Counters
- View the Contents of the Counters

Enable the Counters

The **sampling-enable** command is available at various configuration levels in the CLI. Whenever you see this option, use the **sampling-enable ?** command to view the counters for which you can enable baselining.

For example, see the following configuration where a real server is created:

```
ACOS(config)# slb server s1 2.2.2.2
ACOS(config-real server)# sampling-enable ?
  all          all
  total-conn   Total connections
  fwd-pkt      Forward packets
  rev-pkt      Reverse packets
  peak-conn    Peak connections
ACOS(config-real server)# sampling-enable
```

The counters you will see for the **sampling-enable ?** command will vary depending on the object. You can select specific counters you want to enable or use the **all** keyword to enable all available counters.

The following example enables baselining for three counters under the SLB server configuration, then verifies the configuration with the **show running-config** command:

```
ACOS(config-real server)# sampling-enable total_conn
ACOS(config-real server)# sampling-enable fwd-pkt
ACOS(config-real server)# sampling-enable rev-pkt
ACOS(config-real server)# show running-config | sec slb server
slb server s1 2.2.2.2
  sampling-enable total_conn
  sampling-enable fwd-pkt
  sampling-enable rev-pkt
ACOS(config-real server)#
```

View the Contents of the Counters

To view the values of available counters, use the **show counters** command. This command works the same way even without baselining enabled.

```
ACOS(config-real server-node port)# show counters slb server s1
Current connections                              0
Total connections                                189
Forward packets                                  756
Reverse packets                                  756
Peak connections                                 0
ACOS(config-real server-node port)#
```

The **sampling-enable** command is used to enable enhanced statistical information:

View Counter Baseline Information

To view baseline information, use the **show counters-baselining** command. Note that only the counters for which baselining was enabled with the **sampling-enable** command are listed:

```
ACOS(config-real server-node port)# show counters-baselining slb server
s1

counter_name           min               max               avg
Total Connections      0                 189               66
Forward Packets        0                 756               264
Reverse Packets        0                 756               264
```

```
ACOS(config-real server-node port)#
```

This command shows the minimum, maximum, and average values for each enabled counter over the last 30 seconds.

View Counter Rate Information

To view rate information for each enabled counter, use the **show counters-rate** command. Note that only the counters for which rate information was enabled with the **sampling-enable** command are listed:

```
ACOS(config-real server-node port)# show counters-rate slb server s1

counter_name         1sec_rate         5sec_rate         10sec_rate
30sec_rate
Total connections    0                 0
                18                 6
Forward packets      0                 0                 75
                25
Reverse packets      0                 0                 75
                25
ACOS(config-real server-node port)#
```

This command shows the average value of each counter over the following intervals:

- last second
- last 5 seconds
- last 10 seconds
- last 30 seconds

Session Access Levels

As a security feature, the ACOS operating system separates EXEC sessions into two different access levels – “User EXEC” level and “Privileged EXEC” level. User EXEC level allows you to access only a limited set of basic monitoring commands. The privileged EXEC level allows you to access all ACOS commands (configuration mode, configuration sub-modes, and management mode) and can be password protected to allow only authorized users the ability to configure or maintain the system.

User EXEC Level

The User EXEC level can be identified by the following CLI prompt:

```
ACOS>
```

This is the first level entered when a CLI session begins. At this level, users can view basic system information but cannot configure the system or port parameters.

- A10 Thunder Series models contain “ACOS” plus the model number in the prompt. For example, when an EXEC session is started, the A10 Thunder Series 6430 will display the following prompt:

  ```
  ACOS6430>
  ```

The right arrow (>) in the prompt indicates that the system is at the “User EXEC” level. The User EXEC level does not contain any commands that might control (for example, reload or configure) the operation of the ACOS device. To list the commands available at the User EXEC level, type a question mark (`?`) then press Enter at the prompt; for example,

```
ACOS>?.
```

NOTE: For simplicity, this document uses “ACOS” in CLI prompts, unless referring to a specific model. Likewise, A10 Thunder Series are referred to as “ACOS devices”, since they both run ACOS software.

Privileged EXEC Level

The Privileged EXEC level can be identified by the following CLI prompt:

```
ACOS#
```

This level is also called the “enable” level because the `enable` command is used to gain access. Privileged EXEC level can be password secured. The “privileged” user can perform tasks such as manage files in the flash module, save the system configuration to flash, and clear caches at this level.

Critical commands (configuration and management) require that the user be at the “Privileged EXEC” level. To change to the Privileged EXEC level, type `enable` then press Enter at the `ACOS>` prompt. If an “enable” password is configured, the ACOS

device will then prompt for that password. When the correct password is entered, the ACOS device prompt will change from `ACOS>` to `ACOS#` to indicate that the user is now at the "Privileged EXEC" level. To switch back to the "User EXEC" level, type `disable` at the `ACOS#` prompt. Typing a question mark (`?`) at the Privileged EXEC level will now reveal many more command options than those available at the User EXEC level.

Privileged EXEC Level - Config Mode

The Privileged EXEC level's configuration mode can be identified by the following CLI prompt:

```
ACOS(config)#
```

The Privileged EXEC level's configuration mode is used to configure the system IP address and to configure switching and routing features. To access the configuration mode, you must first be logged into the Privileged EXEC level.

From the opening CLI prompt, enter the following command to change to the Privileged level of the EXEC mode:

```
ACOS> enable
```

To access the configuration level of the CLI, enter the **`config`** command:

```
ACOS# config
```

The prompt changes to include "`(config)`":

```
ACOS(config)#
```

Commands at the Privileged EXEC level are available from configuration mode by prepending the command with do. For example, the clear dns cache command is available in Privileged EXEC mode, while timezone is available in configuration mode. To avoid having to switch configuration levels, like the following example:

```
ACOS(config)# timezone America/Los_Angeles
ACOS(config)# exit
ACOS# clock set 10:30:00 October 1 2015
```

You can use the do command to execute the clock command from configuration mode:

```
ACOS(config)# timezone America/Los_Angeles
ACOS(config)# do clock set 10:30:00 October 1 2015
```

Global Configuration

This reference lists the CLI configuration and show commands that apply specifically to common or global settings for configuring ACOS devices.

Other CLI commands such as DNS Security Extensions (DNSSEC), axDebug, Simple Network Management Protocol (SNMP), System level settings, and common commands (for example, **backup**, **clear**, **debug**, **diff**, **export**, **health-test**, **help**, **import**, **repeat**, **show**, **write**) are also described in this section.

Configuration Commands

Privileged EXEC

The Privileged EXEC mode commands are available at the CLI level that is presented when you enter the **enable** command and a valid enable password from the EXEC level of the CLI.

The Privileged EXEC mode level command prompt ends with #, as in the following example:

```
ACOS#
```

axdebug

Description Enables the axDebug utility to trace packets on the ACOS device.

NOTE: This command is the replacement of the **debug** command.

Syntax **axdebug**

The CLI prompt changes as follows:

```
ACOS(axdebug)#
```

The following are the debug-related commands in the axDebug subsystem:

Parameter	Description
apply-config	Use this command to apply an axDebug configuration file. For more information, see apply-config.
capture	Use this command to start capturing packets. The ACOS device begins capturing packets that match the filter, and saves the packets to a file or displays them, depending on the capture options you specify. For more information, see capture.
file-size	Use this command to change the default size of the capture file. For more information, see file-size.
count	Use this command to change the maximum number of packets to capture. For more information, see count.
delete	Use this command to delete an axDebug capture file. For more information, see delete.
filter-config	Use this command to configure packet filters to match on the types of packets to capture. For more information, see filter-config.
incoming	Use this command to limit the interfaces on which to capture traffic. For more information, see incoming | outgoing.
length	Use this command to save the amount of data in bytes in a pcap file for each packet, if it is larger than that specified number of bytes. For more information, see length.
maxfile	Use this command to specify the maximum number of axDebug packet capture files. For more information, see maxfile.
outgoing	Use this command to limit the interfaces on which to capture traffic. For more information, see incoming | outgoing.
pcapng-config	Use this command to save the capture file in the PCAPNG format. For more information, see pcapng-config.

Parameter	Description
save-config	Use this command to save the axDebug configuration to a file. For more information, see save-config.
sess-filter-dis	Use this command to disable the session-based filter. For more information, see sess-filter-dis.
tcpdump	Use this command to display and filter packets. For more information, see tcpdump.
timeout	Use this command to change the maximum number of minutes during which to capture packets. For more information, see timeout.

Mode axDebug

apply-config

Description Apply an axDebug configuration file.

axDebug configuration files can be created with the save-config command.

Syntax

```
apply-config file
```

Replace *file* with the name of an existing axDebug configuration file (1-63 characters).

Mode axDebug

Example The following example applies the debug configuration saved in the example-ax-debug file:

```
ACOS# axdebug
ACOS(axdebug)# apply-config testfile
Applying debug commands
Done
example-ax-debug has been applied.
ACOS(axdebug)#
```

capture

Description Start capturing packets.

Syntax

```
[no] capture parameter
```

Parameter	Description
brief [**save** ...]	Captures basic information about packets.
detail [**save** ...]	Captures packet content in addition to basic information.
non-display [**save** ...]	Does not display the captured packets on the terminal screen. Use the **save** options to configure a file in which to save the captured packets.
save *filename* [*max-packets*] [**incoming** [portnum ...]] [**outgoing** [portnum ...]]	Saves captured packets in a file: • *filename* – Specifies the name of the packet capture file. • *max-packets* – Specifies the maximum number of packets to capture in the file, 0-65535. To save an unlimited number of packets in the file, specify 0. • **incoming** [*portnum* ...] – Captures inbound packets. You can specify one or more physical Ethernet interface numbers. Separate the interface numbers with spaces. If you do not specify interface numbers, inbound traffic on all physical Ethernet interfaces is captured. • **outgoing** [*portnum* ...] – Captures outbound packets on the specified physical Ethernet interfaces or on all physical Ethernet interfaces. If you do not specify interface numbers, outbound traffic on all physical Ethernet interfaces is captured.

Default By default, packets in both directions on all Ethernet data interfaces are captured.

NOTE: The traffic also must match the AX debug filters.

Mode AX debug

Usage To minimize the impact of packet capture on system performance, it is recommended that you configure an AX debug filter before beginning the packet capture.

To display a list of AX debug capture files or to display the contents of a capture file, refer show axdebug file.

Example The following command captures brief packet information for display on the terminal screen. The output is not saved to a file.

```
ACOS(axdebug)# capture brief
Wait for debug output, enter <ctrl c> to exit
(0,1738448) i( 1,   0, cca8)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 SA 78f07ab8:dbffc02d(0)
(0,1738448) o( 3,   0, cca8)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 SA 78f07ab8:dbffc02d(0)
(0,1738448) i( 1,   0, cca9)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 A 78f07ab9:dbffc0c2(0)
(0,1738448) o( 3,   0, cca9)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 A 78f07ab9:dbffc0c2(0)
(1,1738450) i( 1,   0, ccaa)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 PA 78f07ab9:dbffc0c2(191)
(1,1738450) o( 3,   0, ccaa)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 PA 78f07ab9:dbffc0c2(191)
(1,1738450) i( 1,   0, ccab)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 FA 78f07b78:dbffc0c3(0)
(1,1738450) o( 3,   0, ccab)> ip 10.10.11.30 > 30.30.31.30 tcp
80 > 13632 FA 78f07b78:dbffc0c3(0)
...
```

These lines of debug output show the following:

- 0 – CPU ID. Indicates the CPU that processed the packet. CPU 0 is the control CPU.
- 1738448 – Time delay between packets. This is a jiffies value that increments in 4-millisecond (4-ms) intervals.
- i – Traffic direction: 1 (input) or o (output).
- (1, 0, cca8) – Ethernet interface, VLAN tag, and packet buffer index. If the VLAN tag is 0, then the port is untagged. In this example, the

first packet is received on Ethernet port 1, and the VLAN is not yet known. The packet is assigned to buffer index cca8.

NOTE: Generally, the VLAN tag for ingress packets is 0. It is normal for the ingress VLAN tag to be 0 even when the egress VLAN tag is not 0.

The source and destination IP addresses are listed next, followed by the source and destination protocol port numbers.

The TCP flag is shown next:

- S – Syn
- SA – Syn Ack
- A – Ack
- F – Fin
- PA – Push Ack

The TCP sequence number and ACK sequence number are then shown.

Finally, the packet payload is shown. The header size is excluded.

Example The following command captures packet information and packet contents for display on the terminal screen. The output is not saved to a file.

```
ACOS(axdebug)# capture detail
Wait for debug output, enter <ctrl c> to exit
i( 1, 0, ccae)> ip 10.10.11.30 > 30.30.31.30 tcp 80 > 13638 SA
7ab6ae46:ddb87996(0)
Dump buffer(0xa6657048), len(80 bytes)...
0xa6657048: 00900b0b 3e83001d 09f0dec2 08004500 :
....>.........E.
0xa6657058: 003c0000 40004006 e8580a0a 0b1e1e1e :
.<..@.@..X......
0xa6657068: 1f1e0050 35467ab6 ae46ddb8 7996a012 :
...P5Fz..F..y...
0xa6657078: 16a02ea5 00000204 05b40402 080a5194 :
..............Q.
0xa6657088: 6c551f3c 1d3f0103 03072d59 f97f0000 : lU.<.?....-
Y....
0xa6657098: 00000000 00000000 00000000 00000000 :
................
o( 3, 0, ccae)> ip 10.10.11.30 > 30.30.31.30 tcp 80 > 13638 SA
7ab6ae46:ddb87996(0)
Dump buffer(0xa6657048), len(80 bytes)...
0xa6657048: 001d09f0 e01e0090 0b0b3e83 08004500 :
..........>...E.
0xa6657058: 003c0000 40003f06 e9580a0a 0b1e1e1e :
.<..@.?..X......
0xa6657068: 1f1e0050 35467ab6 ae46ddb8 7996a012 :
...P5Fz..F..y...
0xa6657078: 16a02ea5 00000204 05b40402 080a5194 :
..............Q.
0xa6657088: 6c551f3c 1d3f0103 03072d59 f97f0000 : lU.<.?....-
Y....
0xa6657098: 00000000 00000000 00000000 00000000 :
................
i( 1, 0, ccaf)> ip 10.10.11.30 > 30.30.31.30 tcp 80 > 13638 A
7ab6ae47:ddb87a2b(0)
Dump buffer(0xa6657848), len(80 bytes)...
0xa6657848: 00900b0b 3e83001d 09f0dec2 08004500 :
....>.........E.
0xa6657858: 0034c211 40004006 264f0a0a 0b1e1e1e :
```

```
.4..@.@.&O......
0xa6657868: 1f1e0050 35467ab6 ae47ddb8 7a2b8010 :
...P5Fz..G..z+..
0xa6657878: 00367344 00000101 080a5194 6c561f3c :
.6sD......Q.lV.<
0xa6657888: 1d4041de e3380000 00000000 00000000 :
.@A..8..........
0xa6657898: 00000000 00000000 00000000 00000000 :
................
...
```

Example The following command saves captured packet information in file "file123". The captured traffic is not displayed on the terminal screen.

```
ACOS# axdebug
ACOS(axdebug)# capture save file123
```

count

Description Specify the maximum number of packets to capture.

Syntax

```
count num
```

Replace *num* with the maximum number of packets to capture, 0-65535. To capture an unlimited number of packets, specify 0.

Default 3000

Mode axDebug

Example The following command sets the maximum number of packets to capture to 2048:

```
ACOS# axdebug
ACOS(axdebug)# count 2048
```

delete

Description Deletes an axDebug capture file.

Syntax

```
delete filename
```

Parameter	Description
capture-file	Specify the name of the capture file to delete. The length can be 1-63.
config-file	Specify the name of the config file to delete. The length can be 1-63..

Default N/A

Mode axDebug

Example The following command deletes capture file “file123”:

```
ACOS# axdebug
ACOS(axdebug)# delete file123
```

file-size

Description Specify the size of the axdebug capture file.

Syntax

```
file-size size
```

Replace *size* with the size of the axdebug capture file, between 300 and 6000 in MB.

Default 300 MB

Mode axDebug

Example The following command sets the file size of axdebug capture file to 1000:

```
ACOS# axdebug
ACOS(axdebug)# file-size 1000
```

filter-config

Description Configures an axDebug filter, to specify the types of packets to capture.

Syntax

```
[no] filter filter-id
```

Replace *filter-id* with the ID of the filter (1-32).

This command changes the CLI to the configuration level for the specified axDebug filter, where the following axDebug filter-related commands are available:

Command	Description
dst {**ip** *ipaddr* | **mac** *macaddr* | **port** *portnum*}	Matches on the specified destination IP address, MAC address, or protocol port number.
l3-proto {**arp** | **ip** | **ipv6**}	Matches on the specified Layer 3 protocol.
ip *ipaddr* {*subnet-mask* | **/***mask-length*}	Matches on the specified IPv4 address.
mac *macaddr*	Matches on the specified MAC address.
offset *position* **length** *bytes* *operator value*	Matches on the specified length of bytes and value of those bytes within the packet: • *position* – Starting position within the packet, 0-65535 bytes. • *bytes* – Number of consecutive bytes to filter on, from 0-65535, beginning at the offset position. • *operator* – One of the following: ◦ > (greater than) ◦ >= (greater than or equal to) ◦ <= (smaller than or equal to) ◦ < (smaller than) ◦ = (equal to) • **range** *min-value max-value* (select a range) • *value* – String to filter on.
port *min-portnum*	Matches on the specified range of protocol

Command	Description
max-portnum	port numbers.
proto {**icmp** | **icmpv6** | **tcp** | **udp** | *portnum*}	Matches on the specified protocol or protocol port number.
src {**ip** *ipaddr* | **mac** *macaddr* | **port** *port-num*}	Matches on the specified source IP address, MAC address, or protocol port number.

Default No filters are configured by default. When you create one, all packets match the filter by default.

Mode axDebug

Usage If a packet capture is running and you change the filter, there will be a 5-second delay while the ACOS device clears the older filter. The delay does not occur if a packet capture is not already running.

The packet filter for the **debug** command is internally numbered filter 0. In axDebug, you can create multiple filters, which are uniquely identified by filter ID. If you create filter 0 in axDebug, this filter will overwrite the debug packet filter. Likewise, if you configure filter 0 in axDebug, then configure the **debug** packet filter, the debug packet filter will overwrite axDebug filter 0.

Example The following commands configure an axDebug filter to match on source IP address 10.10.10.30, destination protocol port number 80, and source MAC address aabb.ccdd.eeff. The **show axdebug filter** command displays the filter.

```
ACOS# axdebug
ACOS(axdebug)# filter 1
ACOS(axdebug-filter:1)# src ip 10.10.10.30
ACOS(axdebug-filter:1)# dst port 80
ACOS(axdebug-filter:1)# src mac aabb.ccdd.eeff
ACOS(axdebug-filter:1)# exit
ACOS(axdebug)# show axdebug filter
axdebug filter 1
  src ip 10.10.10.30
```

```
dst port 80
src mac aabb.ccdd.eeff
```

incoming | outgoing

Description Specify the Ethernet interfaces and traffic direction for which to capture packets.

Syntax `[no] incoming [portnum ...] [outgoing [portnum ...]]`

Default Disabled

NOTE: The traffic also must match the axDebug filters.

Mode axDebug

Example The following command limits the packet capture to inbound packets on Ethernet interface 3 and outbound packets on Ethernet interface 4:

```
ACOS# axdebug
ACOS(axdebug)# incoming 3 outgoing 4
```

Example The following command limits the packet capture to outbound packets on Ethernet interface 7. Inbound packets on all Ethernet interfaces are captured, unless specified otherwise in axDebug filters.

```
ACOS# axdebug
ACOS(axdebug)# outgoing 7
```

length

Description Amount of data in bytes to save in a pcap file for each packet, if it is larger than that specified number of bytes.

Syntax `[no] length bytes`

Replace *bytes* with the packet length to capture.

Default 1518 bytes.

Mode axDebug

Example The following command changes the maximum packet length to capture to 137: So if a ping of 5 packets that totals 60 bytes is sent from a peer device, the pcap file would capture 60 bytes. If a ping of 5 packets that totals 1042 bytes is sent from a peer device, the pcap file would capture 137 bytes.

```
ACOS# axdebug
ACOS(axdebug)# length 137
```

maxfile

Description Specify the maximum number of axDebug packet capture files to keep.

Once the maximum is reached, new axDebug files cannot be created until existing files are removed.

Syntax

```
maxfile num
```

Replace *num* with the maximum number of files to keep (1-65535).

Default 100 files

Mode axDebug

Example The following command changes the maximum number of axDebug capture files to keep to 125:

```
ACOS# axdebug
ACOS(axdebug)# maxfile 125
```

pcapng-config

Description Saves the packet capture file in the .pcapng format.

Syntax

```
pcapng-config {pcapng-enable | ssl-key-enable }
```

Parameter	Description
`[no] pcapng-enable`	Enables capturing files in the .pcapng format.
`[no] ssl-key-enable`	Enables SSL key logging in the .pcapng file. It is only valid when the global `pcapng-enable` option is enabled.

Mode axDebug

Usage This feature improves the SSL session tracking and debugging capabilities by saving the pre-master secret key in the .pcapng file.

NOTE: The packet capture feature or command works only with software TLS1.3, QAT, and the new N5 SSL modules.

Limitation When using the `ssl-key-enable` under `pcapng-config`, Wireshark version 3.6.5 (or prior versions) will not show the server certificate key. As a workaround, you must change the following settings in the capture file:
o For HTTPv1/HTTPv2:
Under Analyze Option: Decode As - +TCP port 443 and select HTTP
o For HTTPv3:
Under Analyze Option: Decode As - +UDP port 443 and select HTTP

Example The following example enables the SSL key tracking:

```
ACOS# axdebug
ACOS(axdebug)# pcapng
ACOS(axdebug-pcapng)#ssl-key-enable
```

save-config

Description Saves your axDebug configuration to a file.

This file can be retrieved at a later time with the apply-config command.

Syntax

```
save-config name
```

Replace *name* with the name of the configuration file (1-63 characters).

Mode axDebug

Example The following example saves the axDebug configuration to a file called “example-ax-debug”:

```
ACOS# axdebug
ACOS(axdebug)# save-config example-ax-debug
Config has been saved to example-ax-debug.
ACOS(axdebug)#
```

sess-filter-dis

Description Disables session based filter.

Syntax

```
sess-filter-dis
```

Mode axDebug

Example The following example disables the session based filter:

```
ACOS# axdebug
ACOS(axdebug)# sess-filter-dis
```

tcpdump

Description Use to display and filter packets.

Syntax

```
tcpdump[-AeqStvxX][<expression>]
```

Mode axDebug

Usage You can enable tcpdump's packet display options and filter expressions to display and filter packets.
To display packets, use the various protocol-aware packet printing functions.
To filter packets, use filter expressions.
You can use tcpdump expressions to filter packets and print them.

NOTE:

- vlan is not supported and cannot capture packets based on vlan filter.
- Inbound/ outbound filter is not supported.

Example The following command allows to display and filter packets:

```
ACOS#(axdebug)tcpdump
NAME<length:1-255> Specify tcpdump in quotes ex:"[ -AeqStvxX ]
[ expression ]"
```

```
ACOS(axdebug)#tcpdump "-v host 1.1.1.1"
tcpdump:
02:53:24.442446 IP truncated-ip - 3446 bytes missing! (tos
0x0, ttl 64, id 9305, offset 0, flags [none], proto UDP (17),
length 5028, bad cksum 3eec (->2cec)!)
1.1.1.1.1862 > 1.1.1.2.0: UDP, length 5000

02:53:25.442348 IP truncated-ip - 3446 bytes missing! (tos
0x0, ttl 64, id 39139, offset 0, flags [none], proto UDP (17),
length 5028, bad cksum ca61 (->b861)!)
1.1.1.1.1863 > 1.1.1.2.0: UDP, length 5000

02:53:26.442313 IP truncated-ip - 3446 bytes missing! (tos
0x0, ttl 64, id 9755, offset 0, flags [none], proto UDP (17),
length 5028, bad cksum 3d2a (->ab29)!)
1.1.1.1.1864 > 1.1.1.2.0: UDP, length 5000
```

NOTE: For jumbo packets, the data does not print completely.

timeout

Description Specify the maximum number of minutes to capture packets.

Syntax

```
timeout minutes
```

Replace *minutes* with the number of minutes to capture the packets (0-65535). To save an unlimited number of packets in the file, specify 0.

Default 5 minutes.

Mode axDebug

Example The following command changes the capture timeout to 10 minutes:

```
ACOS# axdebug
ACOS(axdebug)# timeout 10
```

backup log

Description Configure log backup options and save a backup of the system log.

Syntax

```
backup log
  [expedite]
  [period {all | day | month | week | days}]
  [stats-data]
{profile-name | [use-mgmt-port]  url [password password]}
```

Parameter	Description
expedite	Allocates additional CPU to the backup process. This option allows up to 50% CPU utilization to be devoted to the log backup process.
period	Specifies the period of time whose data you want to back up: • **all** - Backs up the log messages contained in the log buffer. • **day** - Backs up the log messages generated during the most recent 24 hours. • **month** - Backs up the log messages generated during the most recent 30 days. • **week** - Backs up the log messages generated during the most recent 7 days. • *days* - Backs up the log messages generated using *days* as the interval (for example, specify 5 to back up every 5 days). The default period of time is one month.
stats-data	Backs up statistical data from the GUI.
profile-name	Profile name for the remote URL. Profiles that can be used in place of the URL are configured with the backup store command.
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device

Parameter	Description
	through a data interface.
url	Specifies the file transfer protocol, the username (if required), and directory path to the location where you want to save the backup file. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]` To enter the entire URL, use one of the following: • **tftp://***host***/***file* • **ftp://**[*user@*]*host*[**:port**]*/file* • **scp://**[*user@*]*host/file* • **sftp://**[*user@*]*host/file*
password	Specifies the password to access the remote site.

Mode Privileged EXEC, or global configuration mode

Usage The **expedite** option controls the percentage of CPU utilization allowed exclusively to the log backup process. The actual CPU utilization during log backup may be higher if other management processes also are running at the same time.

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command backs up statistical data from the GUI:

```
ACOS# backup log stats-data scp://192.168.20.161/log.tgz
```

NOTE: The log **period** and **expedite** settings also apply to backups of the GUI statistical data.

backup system

Description Back up the system. The startup-config file, aFleX policy files, and SSL certificates and keys will be backed up to a `.tar.gz` file.

NOTE: Backing up the system from one hardware platform and restoring it to another is not supported.

Syntax

```
backup system
{profile-name |
[encrypt]
[use-mgmt-port]url
[password password]}
```

Parameter	Description
profile-name	Profile name for the remote URL. Profiles that can be used in place of the URL are configured with the backup store command.
encrypt	Encrypts the backup files. **NOTE:** Use the `encrypt` option to include the non-exportable keys such as the PKI private key in the backup files.
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	The *url* specifies the file transfer protocol, username (if required), and directory path to the location where you want to save the backup file.

Parameter	Description
	You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]` To enter the entire URL, use one of the following: • **tftp://***host***/***file* • **ftp://**[*user@*]*host*[**:port**]*/file* • **scp://**[*user@*]*host/file* • **sftp://**[*user@*]*host/file*
password	Specifies the password to access the remote site.

Default N/A

Mode Privileged EXEC or Global configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example This example backs up the system to the /home/backups folder on host 192.168.2.2.

```
ACOS# backup system tftp://192.168.2.2/home/backups/
```

The trailing slash (/) at the end of the URL tells ACOS that this is a directory path and not a file name. In this case, you'll be prompted for a file name. If no file name is specified, the file name will be automatically generated by ACOS. This is the recommended method of performing

system backups because the file names are guaranteed to be unique. Your backups may fail if you accidentally backup to a file that already exists with the same name.

Example This example backs up the system to a file called “back_file.tar.gz” on host 1.1.1.1:

```
ACOS# backup system tftp://1.1.1.1/back_file
```

clear

Description Clear counters (for example, statistics) or reset processes (for example, Layer 4 sessions).

Syntax

```
clear parameters
```

Default N/A

Mode Privileged EXEC mode or global configuration mode

Example The following example shows the available **clear** options:

```
ACOS# clear s?
  scaleout    Clear scaleout statistics
  sessions    Clear Sessions
  sflow       Clear sFlow related statistics
  slb         Clear SLB related Statistics
  snmp-stats  Clear SNMP Statistics
  statistics  Clear counters on one or all interfaces
  store       Clear store counter
  system      Clear system counter
```

The following example shows the available **clear sessions** options:

```
ACOS# clear sessions ?
  all       Clear all sessions
  diameter  Clear Diameter sessions
  filter    Session filter
  fw        Clear firewall related sessions
  ipv4      Clear ipv4 sessions only
  ipv6      Clear ipv6 sessions only
  persist   Clear Persist sessions
  sip       Clear SIP sessions
  <cr>
```

After entering the **clear session** command, the ACOS device may remain in session-clear mode for up to 10 seconds. During this time, any new connections are sent to the delete queue for clearing.

The following command clears the counters on Ethernet interface 3:

```
ACOS#clear statistics interface ethernet 3
```

Example The following example clears the statistics on trunk interface 100:

```
ACOS#clear statistics interface trunk 100
```

clock

Description Set the system time and date.

Syntax

```
clock set time day month year
```

Parameter	Description
time	Set the time, using 24-hour format hh:mm:ss.
day	Set the day of the month (1-31).
month	Set the month (January, February, March, and so on).
year	Set the year (2013, 2014, and so on).

Mode Privileged EXEC mode

Usage Use this command to manually set the system time and date.

If the system clock is adjusted while OSPF or IS-IS is enabled, the routing protocols may stop working properly. To work around this issue, disable OSPF and IS-IS before adjusting the system clock.

Example Set the system clock to 5:51 p.m. and the date to February 22nd, 2015.

```
ACOS# clock set 17:51:00 22 February 2015
```

configure

Description Enter the configuration mode from the Privileged EXEC mode.

Syntax

```
configure [terminal]
```

Mode Privileged EXEC mode

Example Enter configuration mode.

```
ACOS# configure
ACOS(config)#
```

diff

Description Display a side-by-side comparison of the commands in a pair of locally stored configurations.

Syntax

```
diff {startup-config | profile-name} {running-config | profile-name}
```

Default N/A

Mode Privileged EXEC mode

Usage The following command compares the configuration profile that is currently linked to “startup-config” with the running-config.

```
diff startup-config running-config
```

Similarly, the following command compares the configuration profile that is currently linked to “startup-config” with the specified configuration profile:

```
diff startup-config profile-name
```

To compare a configuration profile other than the startup-config to the running-config, enter the configuration profile name instead of **startup-config**.

To compare any two configuration profiles, enter their profile names instead of **startup-config** or **running-config**.

In the CLI output, the commands in the first profile name you specify are listed on the left side of the terminal screen. The commands in the other profile that differ from the commands in the first profile are listed on the right side of the screen, across from the commands they differ from. The following flags indicate how the two profiles differ:

- | – This command has different settings in the two profiles.
- > – This command is in the second profile but not in the first one.
- < – This command is in the first profile but not in the second one.

disable

Description Exit the Privileged EXEC mode and enter the EXEC mode.

Syntax

```
disable
```

Mode Privileged EXEC mode

Example The following command exits Privileged EXEC mode.

```
ACOS# disable
ACOS>
```

NOTE: The prompt changes from # to >, indicating the change to EXEC mode.

exit

Description Exit the Privileged EXEC mode and enter the EXEC Mode.

Syntax

```
exit
```

Mode Privileged EXEC mode

Example In the following example, the **exit** command is used to exit the Privileged EXEC mode level and return to the User EXEC level of the CLI:

```
ACOS# exit
ACOS>
```

NOTE: The prompt changes from # to >, indicating the change to EXEC mode.

export

Description Puts a file to a remote site using the specified transport method.

Syntax

```
export {filetype filename} [use-mgmt-port] {url | export-store}
```

Parameter	Description
filetype	The following sub-options can be configured:
aflex	Exports an aFleX file.

Parameter	Description
`auth-portal`	Exports an authentication portal file for Application Access Management (AAM).
`auth-portal-image`	Exports the image file for the default portal.
`auth-saml-idp`	Exports the SAML metadata of the identity provider.
`axdebug [merged-pcap | per-cpu | tgz]`	Export an axDebug packet file. By default, the file that is exported will be an uncompressed merge file in PCAP format (without the per-CPU files). To alter this format, use one of the following options: • `merged-pcap` - Export the merge file without the per-CPU files in PCAP format. • `per-cpu` - Include the per-CPU files. • `tgz` - Export the axDebug file without the per-CPU capture files in a `.tgz` format instead of PCAP format.
`bw-list`	Exports a black/white list.
`ca-cert`	Exports a CA cert file.
`cert`	Exports an SSL cert file.
`cert-key`	Exports a certificate and key together as a single file.
`class-list`	Exports an IP class list.
`crl`	Exports a certificate revocation list (CRL).
`csr`	Exports a certificate signing request.
`debug_monitor`	Exports a debug monitor file.
`dnssec-dns-`	Exports a DNSEC key-signing key (KSK) file.

Parameter	Description
`key`	
`dnssec-ds`	Exports a DNSSEC DS file.
`fixed-nat`	Exports the fixed NAT port mapping file.
`fixed-nat-archive`	Exports the fixed NAT port mapping archive file.
`geo-location`	Export the geo-location CSV file.
`health-external`	Export the external program from the system.
`key`	Exports an SSL key file.
`local-uri-file`	Exports the specified image file for the “sorry” page served to RAM Caching clients if all servers are down.
`lw-4o6`	Exports the LW-4over6 binding table file.
`running-config`	Exports the running configuration to a file.
`startup-config` *profile*	Exports the startup configuration.
`store {create` *profile-name* *[options]* | `delete` *profile-name*`}`	Create or delete an export store profile.
`syslog`	Exports the specified syslog file. To export syslog messages, use messages as the filename.
`thales-sec-world`	Exports a Thales security world file.
`visibility`	Export visibility module related files. • `mon-entity-debug` - Export the `mon-entity-debug` file. • `pkt-capture` - Export a pcapng file.

Parameter	Description
`tgz`	Export the axDebug file without the per-CPU capture files in a `.tgz` format instead of PCAP format.
`wsdl`	Exports a Web Services Definition Language (WSDL) file.
`xml-schema`	Exports an XML schema file.
`filename`	Enter the name of the file for the specified file type.
`use-mgmt-port`	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the ACOS device attempts to use the data route table to reach the remote device through a data interface. Protocol, user name (if required), and directory path you want to use to send the file.
`{url | export-store}`	You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: • `tftp://`*`host/file`* • `ftp://[`*`user@`*`]`*`host`*`[:`*`port`*`]/`*`file`* • `scp://[`*`user@`*`]`*`host/file`* • `sftp://[`*`user@`*`]`*`host/file`*

Mode Privileged EXEC mode or global configuration mode

Usage If you omit the final forward slash in the *`url`* string, ACOS attempts to use the string after the final slash as the file name. If you omit the extension, ACOS attempts to use the string after the final slash as the base name of the file. However, this can lead to an error in some cases.

If you are exporting axDebug output, make sure to use the final slash in the *url* string.

Due to a limitation in Windows, it is recommended to use names shorter than 255 characters. Windows allows a maximum of 256 characters for both the file name and the directory path. If the combination of the directory path and file name is too long, Windows will not recognize the file. This limitation is not present on machines running Linux/Unix.

Limitation When exporting a large packet capture from the ACOS GUI, the ACOS CLI may become unresponsive until the export process is completed.

Example The following command exports an aFleX policy from the ACOS device to an FTP server, to a directory named “backups”.

```
ACOS# export aflex aflex-01 ftp://192.168.1.101/backups/aflex-01
```

Example The following command exports the syslog message logs from the ACOS device using scp, with the credential username user1 to a directory named “backups”.

```
ACOS# export syslog messages
scp://user1@192.168.1.101/backups/
```

gen-server-persist-cookie

Description Generate a cookie for pass-through cookie-persistent SLB sessions.

Syntax

```
gen-server-persist-cookie [cookie-name]
match-type
{
  port vport-num rport-num {ipaddr | ipv6 ipv6addr} |
  server {ipv4addr | ipv6 ipv6addr} |
  service-group group-name vport-num rport-num
    {ipv4addr | ipv6 ipv6addr}
}
```

Parameter	Description
cookie-name	Name of the cookie header.

Parameter	Description
port	The **port** option creates a cookie based on the following format: *cookiename-vportnum-groupname=encoded-ip_encoded-rport*
server	The **server** option creates a cookie based on the following format: *cookiename=encoded-ip*
service-group	The **service-group** option creates a cookie based on the following format: *cookiename-vportnum-groupname=encoded-ip_encoded-rport*

Default ACOS does not have a default pass-through cookie. If no name is specified and you configure one, the default name is encrypted.

Mode EXEC and Privileged EXEC only

Usage Additional configuration is required. The **pass-thru** option must be enabled in the cookie-persistence template bound to the virtual port.

health-test

Description Test the status of a device using a configured health monitor.

Syntax

```
health-test {ipaddr | ipv6 ipv6addr}
[count num] [monitorname monitor-name] [port port-num]
```

Parameter	Description
ipaddr	Specifies the IPv4 address of the device to test.
ipv6addr	Specifies the IPv6 address of the device to test.
count *num*	Specifies the number of health checks to send to the device. The default count is 1.
monitor-	Specifies the name of the health monitor you want

Parameter	Description
name	to use. The health monitor must already be configured. The default monitor is ICMP ping, which is the default Layer 3 health check.
port-num	Specifies the protocol port to test. The default is the override port number set in the health monitor configuration. If none is set there, then this option is not set by default.

Mode All

Usage If an override IP address and protocol port are set in the health monitor configuration, the ACOS device will use the override address and port, even if you specify an address and port with the **health-test** command.

Example The following command tests port 80 on server 192.168.1.66, using configured health monitor hm80:

```
ACOS# health-test 192.168.1.66 monitorname hm80
node status UP.
```

Related Commands:

- health monitor

help

Description Display a description of the interactive help system of the ACOS device.

For more information, see Using the Help Command.

Syntax

```
help
```

import

Description Get a file from a remote site.

Syntax

```
import file-type options
```

Parameter	Description
aflex *file_options1*	Import an aFleX file. **Syntax:** **aflex** *filename* {[**user-tag** *user-tag-name*] [**proxy** *host:port*] [**overwrite**] [**use-mgmt-port**] {*url* | *import-store-name* | **terminal**} **Parameters:** • *filename* - local file name (1-63 characters) • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the aFleX file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. • **overwrite** - Enables the overwriting of existing files of the same local name. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
auth-jwks *file_options1*	Import a JSON web key file for Application Access Management (AAM).

Parameter	Description
	For the *file_options1* syntax, see **aflex** *file_options1*.
auth-portal *file_options1*	Import an authentication portal file for Application Access Management (AAM). For the *file_options1* syntax, see **aflex** *file_options1*.
auth-portal-image *file_options1*	Import an image file for the default authentication portal. For the *file_options1* syntax, see **aflex** *file_options1*.
auth-saml-idp *file_options2*	Import the SAML metadata of the identity provider. **Syntax:** **auth-saml-idp** *metadata-name* [**verify-xml-signature**] [**proxy** *host:port*] [**overwrite**] [**use-mgmt-port**] *url* **Parameters:** • *metadata-name* - Local SAML metadata name (1-63 alphanumeric characters) • **verify-xml-signature** - Verify metadata's XML signature • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the SAML metadata file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, [a:b::1]:8080

Parameter	Description
	◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - Enables the overwriting of existing metadata of the same local name • **use-mgmt-port** - See use-mgmt-port below. • *url* - See *url* below.
bw-list *file_options1*	Import a black/white list. For the *file_options1* syntax, see **aflex** *file_options1*.
ca-cert *file_options3*	Imports a CA certificate without a key. ACOS distinguishes between a *CA cert* and an *SSL cert* which is imported using the syntax **cert** *file_options3*. CA certs are not used for handshaking with SSL clients. **Syntax:** **ca-cert {bulk |** *filename*} [**certificate-type** {**pem** | **der** | **pfx** | **p7b**}] [pfx-password *pswd*] **[overwrite] [user-tag** *user-tag-name*] **[use-mgmt-port]** {*url* | *import-store-name* | **terminal}** **Parameters:** • Use the **bulk** option to import multiple files simultaneously as a .tgz archive. ◦ *filename* - local file name (1-255 alphanumeric characters) • Use **certificate-type** {**pem** | **der** | pfx | **p7b**} to specify a certificate type. • Use pfx-password *pswd* to specify the PFX certificated password if and only if you have specified the **pfx** certificate type.

Parameter	Description
	• **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. The **overwrite** option enables the overwriting of an existing bulk file or an existing file of the same local name. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See url below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
cert *file_options3*	Imports an SSL certificate file. ACOS distinguishes between a *CA cert* and an *SSL cert* which is imported using the syntax **ca-cert** *file_options3*. ACOS uses SSL certs and private keys to create proxied signed certificates for handshaking with SSL clients. SSL certs are self-signed by a private organization acting as their own CA. The organization configures its SSL clients to accept its CA. See **ca-cert** *file_options3* for information on *file_options3*.
cert-key *file_options4*	Imports a certificate and key together as a single file. **Syntax:** **cert-key bulk** [pfx-password *pswd*] [**user-tag** *user-tag-name*] [**overwrite**] **[use-mgmt-port]** {*url* | *import-store-name* | **terminal}** **Parameters:**

Parameter	Description
	• Use the **bulk** option to import multiple files simultaneously as a .tgz archive. • Use pfx-password *pswd* to specify the PFX certificated password if and only if the certificate type is **pfx**. • **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. The **overwrite** option enables the overwriting of an existing cert-key bulk file. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See url below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
class-list *file_options1*	Import an IP class list. For the *file_options1* syntax, see **aflex** *file_options1*.
class-list-convert *file_options5*	ACOS imports a newline delimited text file and converts it to a class-list file of the specified type: **Syntax:** **class-list-convert** *filename* class-list-type {ac | string |ipv4 | ipv6 | string-case-intensive} [**user-tag** *user-tag-name*] [**proxy** *host:port*] [**overwrite**] [use-mgmt-port] {*url* | *import-store-name* | **terminal**} **Parameters:** • *filename* – local file name. (1 - 63 characters)

Parameter	Description
	• `class-list-type` - type of class list: • **`ac`** - Aho-Corasick class list. See the "How to Convert Your SNI List to an A10 Class List" section in the *SSL Insight* book for an example of converting to an A10 Aho-Corasick class list. • *`string`* - string class list • **`ipv4`** - ipv4 class list • **`ipv6`** - ipv6 class list • **`string-case-insensitive`** - string case insensitive class list **NOTE:** Only the Aho-Corasick class list is compliant with the class list types created through the `class-list` command. • **`user-tag`** *`user-tag-name`* - Custom tag that can then be searched by using the aXAPI. • **`proxy`** *`host:port`* - Specifies explicit HTTP proxy settings for downloading the class list file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *`[a:b::1]:8080`*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **`overwrite`** - Enables the overwriting of an existing file of the same local name. • **`use-mgmt-port`** – See use-mgmt-port below. • *`url`* – See *url* below.

Parameter	Description
	• *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
crl *file_options1*	Import an SSL certificate revocation list (CRL). For the *file_options1* syntax, see **aflex** *file_options1*. The CRL file name can be from 1 to 255 characters. **NOTE:** When traffic is flowing, the process of loading a large CRL file will consume a significant amount of time. It is recommended to load large CRL files before the initiation of traffic or during maintenance periods. Additionally, frequent updates of large CRL files should be avoided.
dnssec-dnskey *file_options1*	Import a DNSEC key-signing key (KSK) file. For the *file_options1* syntax, see **aflex** *file_options1*. The DNSSEC DNSKEY (KSK) file name can be from 1 to 127 characters.
dnssec-ds *file_options1*	Import a DNSSEC DS file. For the *file_options1* syntax, see **aflex** *file_options1*. The DNSSEC DS file name can be from 1 to 127 characters.
file-inspection-bw-list *file_options1*	Import a Cylance black and white list from Cylance which lists files that were determined to either be good or bad through additional qualification means outside the Cylance machine learning algorithm. **Syntax:** **file-inspection-bw-list** [use-mgmt-port]

Parameter	Description
	Parameters: **use-mgmt-port** - See use-mgmt-port below.
geo-location *file_options1*	Imports a geo-location data file for Global Server Load Balancing (GSLB). For the *file_options1* syntax, see **aflex** *file_options1*.
glm-cert *file_options1*	Imports an global license manager (GLM) certificate. For the *file_options1* syntax, see **aflex** *file_options1*.
glm-license *file_options1*	Imports an activation key license file provided by the global license manager (GLM). For the *file_options1* syntax, see **aflex** *file_options1*.
health-external *file_options6*	Import an external health monitor program. Importing external health monitor scripts is only supported for administrative users provisioned with health monitor (hm) privilege. If commands with this parameter fail due to insufficient privilege, contact your ACOS root administrator. For more information, see the *Application Delivery and Server Load Balancing Guide* (*Using External Health Methods* section) and the *Management Access and Security Guide*. **Syntax:** **health-external** *program-name* **[description** *function*] [proxy host:port] **overwrite**] [use-mgmt-port] *url* **Parameters:**

Parameter	Description
	• *program-name* – local health monitor program name. (1 - 31 characters) • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the external health monitor file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, [a:b::1]:8080 ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - Enables the overwriting of an existing program of the same local name • Use the **description** *function* option to provide a brief description (1-63 characters) of the program purpose or function. • **use-mgmt-port** – See use-mgmt-port below. *url* – See *url* below. **Security Notes:** External health monitors run on a system-level basis at escalated privilege within the ACOS, independent of partition-level constraints. Importing their underlying scripts represents an avenue for potentially malicious code to be introduced into the ACOS system which could be used to compromise the security of the ACOS system or its connected environment. To better ensure confidentiality, integrity, and

Parameter	Description
	availability in an ACOS installation, external health monitor scripts should be carefully reviewed and audited to verify their contents are for the intended monitoring purpose and are free of unsanctioned or untrusted code.
health-postfile *file_options7*	Import the health monitor HTTP post data file. **Syntax**: **health-postfile** *filename* **[proxy** *host:port***]** **[overwrite]** **[use-mgmt-port]** *url* **Parameters**: • *filename* – local health monitor HTTP post data filename. (1 - 31 characters) • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the HTTP post data file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - Enables the overwriting of an existing file of the same local name • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below.
ip-map-list *file_options1*	IP Map List file For the *file_options1* syntax, see **aflex** *file_options1*

Parameter	Description
key *file_options8*	Import the SSL key file. **Syntax:** **key {bulk |** *filename*} [**user-tag** *user-tag-name*] [**overwrite**] [use-mgmt-port] {*url* | *import-store-name* | **terminal}** **Parameters:** • Use the **bulk** option to import multiple files simultaneously as a .tgz archive. • *filename* - local file name (1-255 alphanumeric characters) • **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. • The **overwrite** option enables the overwriting of an existing file of the same local name • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
local-uri-file *file_options1*	Import the local URI files for HTTP responses. For the *file_options1* syntax, see **aflex** *file_options1*
lw-4o6 *file_options1*	Import the LW-4over6 binding table file. For the *file_options1* syntax, see **aflex** *file_options1*
ng-waf-custom-page *html_file*	Import the custom HTML file for Next Generation WAF (NGWAF). **Syntax:**

Parameter	Description
	ng-waf-custom-page *html_file* **{[proxy** *host:port* **] | [overwrite] | [use-mgmt-port]{***url***} }** **Parameters:** • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the HTML file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080* ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - option enables overwriting the existing file of the same local name. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. **NOTE**: The HTML file size should not exceed 100 KB.
ng-waf-module	Import the Next Generation WAF (NGWAF) module. **Syntax:** **ng-waf-module {[proxy** *host:port***] | [overwrite] | [use-mgmt-port]{***url***} }** **Parameters:** • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the NGWAF module. The parameter supports using IPv4, IPv6, or

Parameter	Description
	hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. **NOTE**: The NG-WAF module can be downloaded only from the following url, https://dl.signalsciences.net/sigsci-agent/sigsci-agent_latest.tar.gz
rzp	Refer to import rpz for details.
tsig*file_ options1*	Import the Trasaction Signature (TSIG) key file. The key can be private or public. **Syntax:** **tsig** *filename* {[**user-tag** *user-tag-name*] [**overwrite**] [**use-mgmt-port**] {*url* | *import-store-name* }**}** **Parameters:** • *filename* – local file name (1-63 characters) • **user-tag** *user-tag-name* – Custom tag that can then be searched by using the aXAPI. • The **overwrite** option enables overwriting the existing file of the same local name • **use-mgmt-port** – See use-mgmt-port below.

Parameter	Description
	• *url* – See *url* below. • *import-store-name*- Name of a file stored on ACOS drive memory.
store *file_options9*	Import a storage name for a remote URL. • **store {create** *profile-name url* **| delete** *profile-name***}** • Use **create** to create an import store profile • Use **delete** to delete an import store profile • *profile-name* – name of the ACOS profile to store the remote URL (1 - 31 characters) • *url* – See *url* below.
thales-secworld *file_options1*	Import a Thales security world file. For the *file_options1* syntax, see **aflex** *file_options1*
usb-license *file_options1*	Imports an activation key license file provided from a USB Key. For the *file_options1* syntax, see **aflex** *file_options1*.
web-category-license *file_options1*	Import a web-category-license file, which is required if you wish to access the BrightCloud server and use the web-categorization feature. For the *file_options1* syntax, see **aflex** *file_options1*
wsdl *file_options1*	Import a WSDL file. For the *file_options1* syntax, see **aflex** *file_options1*
xml-schema *file_options1*	Import an XML schema file. For the *file_options1* syntax, see **aflex** *file_*

Parameter	Description
	options1
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	Protocol, user name (if required), and directory path you want to use to send the file. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. The following special characters are supported: • **tftp** - No password required • **ftp** - `!#$%()*+,.: []^_`\|~=` • **scp** - `!#$%()*+,-.:;[]^_`{}|~=` • **http** - `!$%()*+,-.: []^_`{}\|~=` • **https** - `!$%()*+,-.: []^_`{}|~=` • **sftp** - `!#$()*+,-.;=^_`{|}~[]`  The following special characters are not supported:  • **tftp** - No password required • **scp** - All are supported • **ftp** - `-;{}` • **http** - `#;`

Parameter	Description

	• **https** - #;
	• **sftp** - %:
	Syntax:
	{
	tftp://*host/file* |
	ftp://[*user@***]***host*[:*port*]**/***file* |
	scp://[*user@***]***host/file* |
	http://[*user@***]***host/file* |
	https://[*user@***]***host/file* |
	sftp://[*user@***]***host/file* |
	}
	Parameters:
	file - remote file name
	NOTE:
	• This command can be executed only in the shared partition.
	• In case of **http/https** URL, you must replace ? with %3F.
	For example: For **import geo-location aa use-mgmt-port** https://geoblocklist.com/getblocklist.php **?**licenseKey=T3GVxx1Y use **import geo-location aa use-mgmt-port** https://geoblocklist.com/getblocklist.php **%3F**licenseKey=T3GVxx1Y

Syntax Privileged EXEC mode or global configuration mode

Example The following command imports an aFleX policy onto the ACOS device from a TFTP server, from its directory named “backups”:

```
ACOS# import aflex aflex-01
tftp://192.168.1.101/backups/aflex-01
```

Example The following command imports an RPZ file onto the ACOS device:

```
ACOS# import rpz A10.rpz use-mgmt-port
scp://root@192.168.93.182/root/A10.rpz
```

Example The following command imports an NGWAF agent:

```
ACOS# import ng-waf-module
https://dl.signalsciences.net/sigsci-agent/sigsci-agent_
latest.tar.gz
```

Example The following command imports an NGWAF agent using HTTP proxy settings:

```
ACOS(config)# import ng-waf-module proxy [2001:db8::1]:3128
https://dl.signalsciences.net/sigsci-agent/sigsci-agent_
latest.tar.gz
```

Example The following command imports a custom HTML page for NGWAF:

```
ACOS# import ng-waf-custom-page mypage
scp://hostname@192.168.1.101/ngwaf/index.html
```

Example The following command imports a custom HTML page for NGWAF using HTTP proxy settings:

```
ACOS(config)# import ng-waf-custom-page mypage proxy
myproxy.com:443 https://www.google.com
```

Example The following command imports the TSIG private key file:

```
ACOS# import tsig Krpz.com.+157+20696.private use-mgmt-port
scp://root@192.168.93.182/root/Krpz.com.+157+20696.private
```

Example The following command imports a JSON web key file:

```
ACOS# import auth-jwks jwks_file
scp://root@192.168.93.182/root/jwks_file
```

locale

Description Set the locale for the current terminal session.

Syntax

```
locale parameter
```

The following table shows valid values for *parameter*:

Parameter	Description
test	Test the current terminal encodings for a specific locale.
en_US.UTF-8	English locale for the USA, encoding with UTF-8 (default)
zh_CN.UTF-8	Chinese locale for PRC, encoding with UTF-8
zh_CN.GB18030	Chinese locale for PRC, encoding with GB18030
zh_CN.GBK	Chinese locale for PRC, encoding with GBK
zh_CN.GB2312	Chinese locale for PRC, encoding with GB2312
zh_TW.UTF-8	Chinese locale for Taiwan, encoding with UTF-8
zh_TW.BIG5	Chinese locale for Taiwan, encoding with BIG5
zh_TW.EUCTW	Chinese locale for Taiwan, encoding with EUC-TW
ja_JP.UTF-8	Japanese locale for Japan, encoding with UTF-8
ja_JP.EUC-JP	Japanese locale for Japan, encoding with EUC-JP

Default en_US.UTF-8

Mode Privileged EXEC mode or Global Configuration mode

Usage Use this command to configure the locale or to test the supported locales.

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following commands test the Chinese locales and set the locale to zh_CN.GB2312:

```
ACOS(config)# locale test zh_CN
ACOS(config)# locale zh_CN.GB2312
```

no

Description Negate a command or set it to its default setting.

Syntax

```
no command
```

Mode All

Example The following command disables the terminal command history feature:

```
ACOS# no terminal history
ACOS#
```

ping

Description Send an ICMP echo packet to test network connectivity.

Syntax

```
ping [ipv6] {hostname | ipaddr} [use-mgmt-port]
[data HEX-word]
[ds-lite {[source-ipv4  ipaddr] [source-ipv6  ipaddr]
[ipaddr]}]
[flood]
[interface {ethernet port-num | ve ve-num}]
ipv6
[pmtu}
[repeat {count | unlimited}]
[size  num]
[source {ipaddr | ethernet  port-num | ve ve-num}]
[timeout  secs]
[ttl  num]
```

Parameter	Description
ipv6 {*hostname* | *ipaddr*}	Send a ping to the specified IPv6 hostname or address.
[use-mgmt-port]	Use the management port for sending the ping.
{*hostname*	Send a ping to the specified IPv4 hostname or address.

Parameter	Description
| *ipaddr*}	
data *HEX-word*	Hexadecimal data pattern to send in the ping. The pattern can be 1-8 hexadecimal characters long. This is not set by default.
ds-lite { [**source-ipv4** *ipaddr*] [**source-ipv6** *ipaddr*] *ipaddr*}	Send a DS-Lite ping.
flood	Send a continuous stream of ping packets, by sending a new packet as soon as a reply to the previous packet is received. This is disabled by default.
interface { **ethernet** *port-num* **ve** *ve-num*}	Use the specified interface as the source of the ping. Use **ethernet** for ethernet interfaces, or **ve** for virtual ethernet interfaces. By default, this is not set. The ACOS device looks up the route to the ping target in the main route table and uses the interface associated with the route. (The management interface is not used unless you specify the management IP address as the source interface.)
pmtu	Enable PMTU discovery.
repeat {*count* | **unlimited**}	Number of times to send the ping. You can specify a number or specify **unlimited** to ping continuously. The default count is 5.
size *num*	Specify the size of the datagram in bytes. The default size is 84 bytes.

Parameter	Description
source { *ipaddr* | **ethernet** *port-num* | **ve** *ve-num*}	Forces the ACOS Device to give the specified IP address (*ipaddr*), or the IP address configured on the specified interface (either **ethernet** *port-num* or **ve** *ve-num*), as the source address of the ping.
timeout *secs*	Number of seconds the ACOS device waits for a reply to a sent ping packet. The default timeout value is 10 seconds.
ttl *num*	Maximum number of hops the ping is allowed to traverse. The default is 1.

Mode EXEC, Privileged EXEC, and global configuration

Usage The **ping** command sends an echo request packet to a remote address and then awaits a reply. Unless you use the **flood** option, the interval between sending each ping packet is 1 second. It is used to diagnose basic network connectivity.

To terminate a ping session, type ctrl+c.

Example The following command sends a ping to IP address 192.168.3.116:

```
ACOS> ping 192.168.3.116
PING 192.168.3.116 (192.168.3.116) 56(84) bytes of data
64 bytes from 192.168.3.116: icmp_seq=1 ttl=128 time=0.206 ms
64 bytes from 192.168.3.116: icmp_seq=2 ttl=128 time=0.260 ms
64 bytes from 192.168.3.116: icmp_seq=3 ttl=128 time=0.263 ms
64 bytes from 192.168.3.116: icmp_seq=4 ttl=128 time=0.264 ms
64 bytes from 192.168.3.116: icmp_seq=5 ttl=128 time=0.216 ms
--- 192.168.3.116 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.206/0.241/0.264/0.032 ms
```

Example The following command sends a ping to IP address 10.10.1.20, from ACOS Ethernet port 1. The ping has a data pattern "ffff", which is 1024 bytes long and is sent 100 times.

```
ACOS> ping data ffff repeat 100 size 1024 source ethernet 1
10.10.1.20
```

reboot

Description Reboot the ACOS Device.

Syntax

```
reboot [
all |
text |
in hh:mm [text] |
at hh:mm [month day | day month] [text] |
cancel
]
```

Parameter	Description
all	Reboot all devices when VCS is enabled, or only this device itself if VCS is not enabled.
text	Reason for the reboot.
in *hh:mm*	Schedule a reboot to take effect in the specified hours and minutes. The reboot must take place within approximately 24 hours.
at hh:mm	Schedule a reboot to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reboot is scheduled to take place at the specified time and date. If you do not specify the month and day, the reboot takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reboot for midnight.
month	Name of the month, any number of characters in a unique string.
day	Number of the day.
cancel	Cancel a scheduled reboot.

Mode Privileged EXEC mode

Usage The **reboot** command halts the system. If the system is set to restart on error, it reboots itself. Use the **reboot** command after configuration information is entered into a file and saved to the startup configuration.

You cannot reboot from a virtual terminal if the system is not set up for automatic booting. This prevents the system from dropping to the ROM monitor and thereby taking the system out of the remote user's control.

If you modify your configuration file, the system will prompt you to save the configuration.

The **at** keyword can be used only if the system clock has been set on the ACOS device (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the ACOS device. To schedule reboots across several ACOS devices to occur simultaneously, the time on each ACOS device must be synchronized with NTP. To display information about a scheduled reboot, use the **show reboot** command.

Example The following example immediately reboots the ACOS device:

```
ACOS# reboot
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
Write configuration to default primary startup-config


...
Proceed with reboot? [yes/no]: yes
```

Example The following example reboots the ACOS Device in 10 minutes:

```
ACOS# reboot in 00:10
Proceed with reboot? [yes/no] yes
ACOS#
```

Example The following example reboots the ACOS Device at 1:00 p.m. today:

```
ACOS# reboot at 13:0013:00
Proceed with reboot? [yes/no] yes
```

```
ACOS#
```

Example The following example reboots the ACOS Device on Apr 20 at 4:20 p.m.:

```
ACOS# reboot at 16:20 april 20
Proceed with reboot? [yes/no] yes
ACOS#
```

Example The following example cancels a pending reboot:

```
ACOS# reboot cancel
***
*** --- SHUTDOWN ABORTED ---
***
```

reload

Description Restart ACOS system processes and reload the startup-config, without rebooting.

Syntax **reload [all | device** *device-id*]

Parameter	Description
all	When VCS is enabled, this parameter causes all devices in the virtual chassis to be reloaded. When VCS is disabled, this parameter causes only the device on which this command is run to be reloaded.
device-id	When VCS is enabled, this parameter causes only the specified device to be reloaded. When VCS is disabled, this parameter will return an error message.

Mode Privileged EXEC mode

Usage The **reload** command restarts ACOS system processes and reloads the startup-config, without reloading the system image. To also reload the system image, use the **reboot** command instead.

The ACOS Device closes all sessions as part of the reload.

If the **reload** command is used without any optional parameters then only the device on which the command is run will be reloaded. This is the case for both VCS-enabled and VCS-disabled devices.

Example Below is an example of the **reload** command:

```
ACOS# reload

Do you wish to proceed with reload? [yes/no]:yes
System is reloading now. Please wait ....

System has reloaded successfully.
ACOS#
```

Related Commands:

- reboot

repeat

Description Periodically re-enter a **show** command.

Syntax **repeat** *seconds* **show** *command-options*

Parameter	Description
seconds	Interval at which to re-enter the command.
command-options	Options of the **show** command.

Mode Privileged EXEC mode

Usage The **repeat** command is especially useful when monitoring or troubleshooting the system.

The elapsed time indicates how much time has passed since you entered the **repeat** command. To stop the command, press Ctrl+C.

shutdown

Description Schedule a system shutdown at a specified time or after a specified interval, or cancel a scheduled system shutdown.

Syntax **shutdown** {**at***hh*:*mm*| **in***hh*:*mm* | **cancel** [*text*]}

Parameter	Description
at	Schedule a reboot to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reboot is scheduled to take place at the specified time and date. If you do not specify the month and day, the reboot takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reboot for midnight.
in	Shutdown after a specified time interval (*hh:mm*). For example, `00:10` causes the device to shut down 10 minutes from now.
cancel	Cancel pending shutdown
text	Reason for shutdown

Mode Privileged EXEC mode

Example The following command schedules a system shutdown to occur at 11:59 p.m.:

```
ACOS# shutdown at 23:59

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Shutdown scheduled for 23:59:00 UTC Fri Sep 30 2005 (in 5
hours and 39 minutes) by admin on 192.168.1.102
Proceed with shutdown? [confirm]
ACOS#
```

Example The following command cancels a scheduled system shutdown:

```
ACOS# shutdown cancel
***
*** --- SHUTDOWN ABORTED ---
***
```

ssh

Description Establish a Secure Shell (SSH) connection from the ACOS device to a different device.

Syntax

```
ssh [use-mgmt-port] {hostname | ipaddr} login-name [protocol-port]
```

Parameter	Description
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the ACOS Device attempts to use the data route table to reach the remote device through a data interface.
hostname	Host name of the remote system.
ipaddr	IP address of the remote system.
login-name	The user name used to log in to the remote system.
protocol-port	TCP port number on which the remote system listens for SSH client traffic. The default port is 22.

Mode EXEC and Privileged EXEC

Usage SSH version 2 is supported. SSH version 1 is not supported. SSH from the ACOS device to a different device is not supported from the shared VLAN in a private partition on a VRRP-A standby device unless it is used in the following manner: **ip mgmt-traffic ssh source-interface source-ip a.b.c.d**, where a.b.c.d is the shared VLAN interface.

telnet

Description Open a Telnet tunnel connection from the ACOS device to another device.

Syntax

```
telnet [use-mgmt-port] {hostname | ipaddr) [protocol-port]
```

Parameter	Description
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
hostname	Host name of the remote system.
ipaddr	IP address of the remote system.
protocol-port	TCP port number on which the remote system listens for Telnet traffic. The default port is 23.

Mode EXEC and Privileged EXEC

Example The following command opens a Telnet session from one ACOS device to another ACOS device at IP address 10.10.4.55:

```
ACOS> telnet 10.10.4.55
Trying 10.10.4.55...
Connected to 10.10.4.55.
Escape character is '^]'.
Welcome to Thunder
ACOS login:
```

terminal

Description Set terminal display parameters for the current session.

Syntax

```
terminal
{
auto-size |
command-timestamp [unix]|
editing |
gslb-prompt options |
history [size number] |
length number |
monitor |
width lines
}
```

Parameter	Description
auto-size	Enables the terminal length and width to automatically change to match the terminal window size. This is enabled by default.
command-timestamp	Include timestamp information in the **show** command output. The **unix** option displays the timestamp in Unix format (`sec.us`) since Unix Epoch.
editing	Enables command-line editing. This is enabled by default.

gslb-prompt *options*	Enables the CLI prompt to display the role of the ACOS device within a GSLB group.
	
	• **disable** - disables this feature so the CLI prompt does not display role information
	
	• **group-role** - displays “Member” or “Master” in the CLI prompt. For example:
	
	`ACOS:Master(config)#`
	
	• **symbol** - displays “gslb” in the CLI prompt after the name of the ACOS device. For example:
	
	`ACOS-gslb:Master(config)#`

history [*size*]	Enables and controls the command history function. The *size* option specifies the number of command lines that will be held in the history buffer. This is enabled by default.
length *num*	Sets the number of lines on a screen. Specifying 0 disables pausing.
monitor	Copies debug output to the current terminal. This is disabled by default.

Parameter	Description
width *num*	Sets the width of the display terminal. The setting 0 means “infinite”.

Mode Privileged EXEC mode

Usage This command affects only the current CLI session. The command is not added to the running-config and does not persist across reloads or reboots. To make persistent changes, use the command at the global configuration level.

Example The following command changes the terminal length to 40:

```
ACOS# terminal length 40
```

Example The following example shows the **command-timestamp** option. Note the “Command start time” and “Command end time” lines added as the first and last lines of the output:

```
ACOS# terminal command-timestamp
ACOS# show config-block
Command start time : 1422647248.076561
!Block configuration:   24 bytes
!64-bit Advanced Core OS (ACOS) version 4.1.1-P1, build 17
(Nov-15-2016,05:35)
!
interface ethernet 1
!
!
end
!Configuration specified in merge mode
Command end time : 1422647248.077418
ACOS#
```

Related Commands:

- terminal

traceroute

Description Display the router hops through which a packet sent from the ACOS device can reach a remote device.

Syntax

```
traceroute [ipv6 | use-mgmt-port] {hostname | ipaddr}
```

Parameter	Description
ipv6	Indicates that the remote device is an IPv6 system.
use-mgmt-port	Uses the management interface as the source interface. The management route table is used to reach the device. By default, the ACOS Device attempts to use the data route table to reach the remote device through a data interface.
hostname	Host name of the device at the remote end of the route to be traced.
ipaddr	IP address of the device at the remote end of the route to be traced.

Default N/A

Mode EXEC and Privileged EXEC

Usage If a hop does not respond within 5 seconds, asterisks (*) are shown in the row for that hop.

Example The following command traces a route to 192.168.10.99:

```
ACOS> traceroute 192.168.10.99
traceroute to 192.168.10.99 (192.168.10.99), 30 hops max, 40
byte packets
 1  10.10.20.1 (10.10.20.1)  1.215 ms  1.151 ms  1.243 ms
 2  10.10.13.1 (10.10.13.1)  0.499 ms  0.392 ms  0.493 ms
 ...
```

write force

Description Forces the ACOS device to save the configuration regardless of whether the system is ready.

NOTE: Using this command can result in an incomplete or empty configuration! It is recommended that you use this command only with the advice of Technical Support.

Syntax

```
write force [parameters]
```

Parameter	Description
all-partitions	Write the configuration to the pri_default configuration profile stored in all partitions.
primary *[options]*	Write the configuration to the configuration profile stored in the default primary configuration area.
secondary *[options]*	Write the configuration to the configuration profile stored in the default secondary configuration area.
name [options]	Write the configuration to a specified profile name.
options	• **all-partitions** • **cf** • **partition**

Mode Privileged EXEC and Global configuration

Example Force the ACOS Device to save the current configuration to a custom profile called “custom-prof”:

```
ACOS# write force custom-prof
```

write memory

Description Write the running-config to a configuration profile.

Syntax

```
writememory
  [primary | secondary | profile-name]
    [all-partitions | partition {shared | part-name}]
```

Parameter	Description
primary	Replaces the **Default** configuration profile of the primary image area with the running-config. If the

Parameter	Description
	Default profile is not linked and a custom-named profile is linked instead, please run `write memory` or `write memory all-partitions` to ensure that the running-config is saved to the current linked profile This option is only available in L3V partitions for root admin users.
secondary	Replaces the **Default** configuration profile of the secondary image area with the running-config. If the Default profile is not linked and a custom-named profile is linked instead, please run `write memory` or `write memory all-partitions` to ensure that the running-config is saved to the current linked profile. This option is only available in L3V partitions for root admin users.
profile-name	Replaces the commands in the specified configuration profile with the running-config.
all-partitions	Saves changes for all resources in all partitions.
shared	Saves changes only for the resources in the shared partition.
part-name	Saves changes only for the resources in the specified L3V partition.

Default If you enter **write memory** without additional options, the command replaces the configuration profile that is currently linked to by "startup-config" with the commands in the running-config. If startup-config is set to its default (linked to the configuration profile stored in the image area that was used for the last reboot), then **write memory** replaces the configuration profile in the image area with the running-config.

Unless you use the **force** option, the command checks for system readiness and saves the configuration only if the system is ready.

Mode Privileged EXEC and Global configuration

Example The following command saves the running-config to the configuration profile stored in the primary image area of the hard disk:

```
ACOS#write memory primary
Building configuration...
Write configuration to primary default startup-config
Do you also want to write configuration to secondary default
startup-config as well?
 (y/n):y
[OK]
```

Example The following command saves the running-config to a configuration profile named "slbconfig2":

```
ACOS#write memory slbconfig2
```

Example The following command attempts to save the running-config but the system is not ready:

```
ACOS#write memory
ACOS is not ready. Cannot save the configuration.
```

write terminal

Description Display the current running-config on your terminal.

Syntax

```
write terminal
```

Mode Privileged EXEC and Global configuration

Example Example output from this command (output is truncated for brevity):

```
ACOS#write terminal
!Current configuration: 2877 bytes
!Configuration last updated at 03:08:11 IST Tue Jul 7 2015
!Configuration last saved at 04:18:08 IST Tue Jul 7 2015
!version 4.1.1, build 177 (Jun-22-2015,04:56)
!
hostname ACOS
!
clock timezone Europe/Dublin
!
!
```

```
. . .
```

EXEC

The EXEC commands (sometimes referred to as the User EXEC commands) are available at the CLI level that is presented when you log into the CLI.

The EXEC level command prompt ends with >, as in the following example:

```
ACOS>
```

active-partition

Description CLI commands related to ADPs are located in *Configuring Application Delivery Partitions*.

enable

Description Enter privileged EXEC mode, or any other security level set by a system administrator.

Syntax

```
enable
```

Mode EXEC

Usage Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter it before being allowed access to privileged EXEC mode. The password is case sensitive.

The user will enter the default mode of privileged EXEC.

Example In the following example, the user enters privileged EXEC mode using the **enable** command. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is >, and the prompt for privileged EXEC mode is #.

```
ACOS> enable
Password: <letmein>
```

```
ACOS# disable
ACOS>
```

exit

Description When used from User EXEC mode, this command closes an active terminal session by logging off the system. In any other mode, it will move the user to the previous configuration level.

Syntax

```
exit
```

Mode All

Example In the following example, the **exit** command is used three times:

1. To move from Global configuration mode to the previous config level (privileged EXEC mode);
2. To move from privileged EXEC mode to the previous config level (User EXEC mode);
3. From User EXEC mode, the **exit** command is used to log off (exit the active session):

```
ACOS(config)# exit
ACOS# exit
ACOS> exit
Are you sure to quit (N/Y)?: Y
```

help

Description Display a description of the interactive help system of the CLI.

Syntax

```
help
```

Mode All

Example

```
ACOS(config)#help
```

no

Description Negate a command or set it to its default setting.

Syntax

```
no command
```

Mode All

Example The following command disables the terminal command history feature:

```
ACOS# no terminal history
ACOS#
```

show

Description Displays system or configuration information.

Syntax `show options`

Default N/A

Mode All

Global

The Global or system-level command prompt ends with **config #**, as in the following example:

```
ACOS>configure
ACOS(config)#
```

aam

Description For more information, see *Application Access Management Guide*.

access-list (standard)

Description Configures a standard Access Control List (ACL) to permit or deny source IP addresses.

Syntax

```
[no] access-list acl-num [seq-num]
{permit | deny | l3-vlan-fwd-disable | remark string}
{any | host host-ipaddr | src-ipaddr {filter-mask | /mask-length}}
[log  [transparent-session-only]]
```

Parameter	Description
acl-num	Standard ACL number (1-99).
seq-num	Sequence number of this rule in the ACL. You can use this option to re-sequence the rules in the ACL.
permit	Allows traffic for ACLs applied to interfaces or used for management access. For ACLS used for IP source NAT, this option is also used to specify the inside host addresses to be translated into external addresses. **NOTE:** If you are configuring an ACL for source NAT, use the **permit** action. For ACLs used with source NAT, the **deny** action does not drop traffic, it simply does not use the denied addresses for NAT translations.

Parameter	Description
deny	Drops traffic for ACLs applied to interfaces or used for management access.
l3-vlan-fwd-disable	Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
remark*string*	Adds a remark to the ACL. The remark appears at the top of the ACL when you display it in the CLI. **NOTE:** An ACL and its individual rules can have multiple remarks. To use blank spaces in the remark, enclose the entire remark string in double quotes. The ACL must already exist before you can configure a remark for it.
any	Denies or permits traffic received from any source host.
host *host-ipaddr*	Denies or permits traffic received from a specific, single host.
src-ipaddr {*filter-mask* | **/***mask-length*}	Denies or permits traffic received from the specified host or subnet. The *filter-mask* specifies the portion of the address to filter: • Use 0 to match. • Use 255 to ignore. For example, the *filter-mask* 0.0.0.255 filters on a 24-bit subnet. Alternatively, you can use */mask-length* to specify the portion of the address to filter. For example, you can specify "/24" instead "0.0.0.255" to filter on a 24-bit subnet.
log [**transparent-session-only**]	Configures the ACOS device to generate log messages when traffic matches the ACL.

Parameter	Description
	The `transparent-session-only` option limits logging for an ACL rule to creation and deletion of transparent sessions for traffic that matches the ACL rule.

Default No ACLs are configured by default. When you configure one, the `log` option is disabled by default.

Mode Configuration mode

Usage An ACL can contain multiple rules. Each `access-list` command configures one rule. Rules are added to the ACL in the order you configure them. The first rule you add appears at the top of the ACL.

Rules are applied to the traffic in the order they appear in the ACL (from the top, which is the first rule, downward). The first rule that matches traffic is used to permit or deny that traffic. After the first rule match, no additional rules are compared against the traffic.

To move a rule within the sequence, delete the rule, then re-add it with a new sequence number.

Access lists do not take effect until you apply them.

An ACL is used to do the following:

- Filter traffic on an interface. For more information, seeaccess-list command.
- Filter traffic on a virtual server port. For more information, seeaccess-list command.
- Control management access
- Support source NAT. For more information, seeip nat inside source command.

The syntax shown in this section configures a standard ACL, which filters based on source IP address. To filter on additional values such as destination address, IP protocol, or TCP/UDP ports, configure an extended ACL. ()

Support for Non-Contiguous Masks in IPv4 ACLs

A contiguous comparison mask is one that, when converted to its binary format, consists entirely of ones. A non-contiguous mask, however, contains at least one zero. Table 9 shows some examples of IPv4 addresses with each of the ACL mask types, a contiguous mask and a non-contiguous mask. The addresses and masks are shown in both their decimal and binary formats.

The “F” column indicates the format, decimal (D) or binary (B).

Table 9 : IPv4 Address and Mask Examples

F	Address				Mask			
D	10	10	10	0	*0*	255	255	255
B	00001010	00001010	00001010	00000000	*00000000*	11111111	11111111	11111111
D	10	10	10	0	*0*	255	*0*	255
B	00001010	00001010	00001010	00000000	*00000000*	11111111	*00000000*	11111111
D	172	0	3	0	*0*	255	255	255
B	10101100	00000000	00000010	00000000	*00000000*	11111111	11111111	11111111
D	172	0	3	0	*0*	255	*0*	255
B	10101100	00000000	00000010	00000000	*00000000*	11111111	*00000000*	11111111

The non-contiguous masks are shown in italics.

Example The following commands configure a standard ACL and use it to deny traffic sent from subnet 10.10.10.x, and apply the ACL to inbound traffic received on Ethernet interface 4:

```
ACOS(config)# access-list 1 deny 10.10.10.0 0.0.0.255
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# access-list 1 in
```

Example The commands in this example configure an ACL that uses a non-contiguous mask, and applies the ACLto a data interface:

```
ACOS(config)# access-list 3 deny 172.0.3.0 0.255.0.255
```

```
Info: Configured a non-contiguous subnet mask.[1]
ACOS(config)# access-list 20 permit any
ACOS(config)# show access-list
access-list 3 4 deny 172.0.3.0 0.255.0.255  Data plane hits: 0
access-list 20 4 permit any  Data plane hits: 0
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# access-list 3 in
```

Based on this configuration, attempts to ping or open an SSH session with destination IP address 172.17.3.130 from source 172.16.3.131 are denied. However, attempts from 172.16.4.131 are permitted.

Example

This example shows how the sequence numbers in an ACL are re-numbered after reloading or rebooting the device. Consider the following ACL configuration, with sequence numbers 1, 2, and 3:

```
ACOS(config)# access-list 1 1 remark "A test ACL"
ACOS(config)# access-list 1 2 permit ip 192.0.0.0
0.255.255.255 any
ACOS(config)# access-list 1 3 permit ip 172.0.0.0
0.255.255.255 any
```

After the configuration is saved and the device is reloaded or rebooted, the sequence numbers are re-numbered to 4, 8, and 12:

```
ACOS(config)# show access-list
access-list 1 4 remark "A test ACL"
access-list 1 8 permit ip 192.0.0.0 0.255.255.255 any
access-list 1 12 permit ip 172.0.0.0 0.255.255.255 any
```

This makes is easier to introduce new access-list statements in the desired order.

Related Commands:

- access-list (extended)
- disable-management
- enable-management

[1]This message appears a maximum of 2 times within a given CLI session.

access-list (extended)

Description Configures an extended Access Control List (ACL) to permit or deny traffic based on source and destination IP addresses, IP protocol, and TCP/UDP ports.

Syntax

```
[no] access-list  acl-num [seq-num]
{permit | deny | l3-vlan-fwd-disable | remark string} ip

{any | host  host-src-ipaddr | object-group  src-group-name |
net-src-ipaddr {filter-mask | /mask-length}}

{any | host  host-dst-ipaddr | object-group  dst-group-name |
net-dst-ipaddr {filter-mask | /mask-length}}

[fragments] [vlan  vlan-id [ethernet eth-id | trunk trunk-id]]
[dscp  num]

[log [transparent-session-only]]
```

or

```
[no] access-list  acl-num [seq-num]
{permit | deny | l3-vlan-fwd-disable | remark string} icmp

[type icmp-type [code icmp-code]]

{any | host  host-src-ipaddr | object-group  src-group-name |
net-src-ipaddr {filter-mask | /mask-length}}

{any | host  host-dst-ipaddr | object-group  dst-group-name |
net-dst-ipaddr {filter-mask | /mask-length}}

[fragments] [vlan  vlan-id [ethernet eth-id | trunk trunk-id]]
[dscp  num]

[log [transparent-session-only]]
```

or

```
[no] access-list  acl-num [seq-num]
{permit | deny | l3-vlan-fwd-disable | remark string}
object-group svc-group-name

{any | host  host-src-ipaddr | object-group  src-group-name |
net-src-ipaddr {filter-mask | /mask-length}}

{any | host  host-dst-ipaddr | object-group  dst-group-name |
net-dst-ipaddr {filter-mask | /mask-length}}

[fragments] [vlan  vlan-id [ethernet eth-id | trunk trunk-id]]
[dscp  num]

[log [transparent-session-only]]
```

or

```
[no] access-list  acl-num [seq-num]
{permit | deny | l3-vlan-fwd-disable | remark string} {tcp |
udp}

{any | host  host-src-ipaddr | net-src-ipaddr
  {filter-mask | /mask-length}}
  [eq  src-port | gt  src-port | lt  src-port |
  range  start-src-port end-src-port]

{any | host  host-dst-ipaddr | net-dst-ipaddr
  {filter-mask | /mask-length}}
  [eq  dst-port | gt  dst-port | lt  dst-port |
  range  start-dst-port end-dst-port]

[fragments] [vlan  vlan-id [ethernet eth-id | trunk trunk-id]]
[dscp  num][established]

[log [transparent-session-only]]
```

Parameter	Description
acl-num	Extended ACL number (100-199).

Parameter	Description
seq-num	Sequence number of this rule in the ACL. You can use this option to re-sequence the rules in the ACL.
permit	Allows traffic that matches the ACL.
deny	Drop the traffic that matches the ACL.
l3-vlan-fwd-disable	Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
remark ***string***	Adds a remark to the ACL. The remark appears at the top of the ACL when you display it in the CLI. **NOTE:** An ACL and its individual rules can have multiple remarks. To use blank spaces in the remark, enclose the entire remark string in double quotes. The ACL must already exist before you can configure a remark for it.
ip	Filters on IP packets only.
icmp	Filters on ICMP packets only.
tcp | udp	Filters on TCP or UDP packets, as specified. These options also allow you to filter based on protocol port numbers.
object-group	Object group name. Object groups provide additional flexibility in ACL management; they can simplify ACL implementations and extend the ACL number and functionality limitations.
type ***icmp-type***	This option is applicable if the protocol type is **icmp**. Matches based on the specified ICMP type. You can specify one of the following. Enter the type name or the type number (for example, “dest-unreachable” or “3”). • **any-type** – Matches on any ICMP type.

Parameter	Description
	• **dest-unreachable**, or **3** – destination is unreachable. • **echo-reply**, or **0** – echo reply. • **echo-request**, or **8** – echo request. • **info-reply**, or **16** – information reply. • **info-request**, or **15** – information request. • **mask-reply**, or **18** – address mask reply. • **mask-request**, or **17** – address mask request. • **parameter-problem**, or **12** – parameter problem. • **redirect**, or **5** – redirect message. • **source-quench**, or **4** – source quench. • **time-exceeded**, or **11** – time exceeded. • **timestamp**, or **14** – timestamp. • **timestamp-reply**, or **13** – timestamp reply.
code ***icmp-code***	This option is applicable if the protocol type is **icmp**. Matches based on the specified ICMP code. Replace *code-num* with an ICMP code number (0-254), or specify **any-code** to match on any ICMP code.
any | **host** ***host-src-ipaddr*** | ***net-src-ipaddr*** **{** ***filter-mask*** | ***/mask-length*****}**	The source IP addresses to filter. • **any** - the ACL matches on any source IP address. • **host** ***host-src-ipaddr*** - the ACL matches only on the specified host IP address. • ***net-src-ipaddr*** **{*****filter-mask*** | ***/mask-length*****}** - the ACL matches on any host in the specified subnet. The *filter-mask* specifies the portion of the address to filter: ◦ Use 0 to match.

Parameter	Description
	◦ Use 255 to ignore. For example, the ***filter-mask*** 0.0.0.255 filters on a 24-bit subnet. Alternatively, you can use ***/mask-length*** to specify the portion of the address to filter. For example, you can specify "/24" instead "0.0.0.255" to filter on a 24-bit subnet.
eq ***src-port*** | **gt** ***src-port*** | **lt** ***src-port*** | **range** ***start-src-port*** ***end-src-port***	The source protocol ports to filter for TCP and UDP: • **eq** ***src-port*** - The ACL matches on traffic from the specified source port. • **gt** ***src-port*** - The ACL matches on traffic from any source port with a higher number than the specified port. • **lt** ***src-port*** - The ACL matches on traffic from any source port with a lower number than the specified port. • **range** ***start-src-port end-src-port*** - The ACL matches on traffic from any source port within the specified range.
any | **host** ***host-dst-ipaddr*** | ***net-dst-ipaddr*** { ***filter-mask*** | ***/mask-length***}	The destination IP addresses to filter. • **any** - the ACL matches on any destination IP address. • **host** ***host-dst-ipaddr*** - the ACL matches only on the specified host IP address. • ***net-dst-ipaddr*** {***filter-mask*** | ***/mask-length***} - the ACL matches on any host in the specified subnet. The *filter-mask* specifies the portion of the address to filter: ◦ Use 0 to match.

Parameter	Description
	◦ Use 255 to ignore. For example, the ***filter-mask*** 0.0.0.255 filters on a 24-bit subnet. Alternatively, you can use ***/mask-length*** to specify the portion of the address to filter. For example, you can specify "/24" instead "0.0.0.255" to filter on a 24-bit subnet.
eq ***dst-port*** | **gt** ***dst-port*** | **lt** ***dst-port*** | **range** ***start-dst-port*** ***end-dst-port***	The destination protocol ports to filter for TCP and UDP: • **eq** ***src-port*** - The ACL matches on traffic from the specified destination port. • **gt** ***src-port*** - The ACL matches on traffic from any destination port with a higher number than the specified port. • **lt** ***src-port*** - The ACL matches on traffic from any destination port with a lower number than the specified port. • **range** ***start-src-port end-src-port*** - The ACL matches on traffic from any destination port within the specified range.
fragments	Matches on packets in which the More bit in the header is set (1) or has a non-zero offset.
vlan ***vlan-id*** [ethernet *eth-id* | trunk *trunk-id*]	Matches on the specified VLAN. VLAN matching occurs for incoming traffic only. • **ethernet** ***eth-id*** - In a single partition SSLi topology, the Ethernet interfaces are available as selectors in Extended ACLs for directing Layer 2 traffic through specific interface IDs. • **trunk** ***trunk*** -In a single partition SSLi topology, the trunk interfaces are available as selectors in

Parameter	Description
	Extended ACLs for directing Layer 2 traffic through specific interface IDs.
dscp *num*	Matches on the 6-bit Diffserv value in the IP header, 1-63.
established	Matches on TCP packets in which the ACK or RST bit is set. This option is useful for protecting against attacks from outside. Since a TCP connection from the outside does not have the ACK bit set (SYN only), the connection is dropped. Similarly, a connection established from the inside always has the ACK bit set. (The first packet to the network from outside is a SYN/ACK.)
log [transparent-session-only]	Configures the ACOS device to generate log messages when traffic matches the ACL. The **transparent-session-only** option limits logging for an ACL rule to creation and deletion of transparent sessions for traffic that matches the ACL rule.

Default No ACLs are configured by default. When you configure one, the **log** option is disabled by default.

Mode Configuration mode

Usage An ACL can contain multiple rules. Each **access-list** command configures one rule. Rules are added to the ACL in the order you configure them. The first rule you add appears at the top of the ACL.

Rules are applied to the traffic in the order they appear in the ACL (from the top, which is the first, rule downward). The first rule that matches traffic is used to permit or deny that traffic. After the first rule match, no additional rules are compared against the traffic.

To move a rule within the sequence, delete the rule, then re-add it with a new sequence number.

Access lists do not take effect until you apply them.

An ACL is used to do the following:

- Filter traffic on an interface. For more information, see access-list command.
- Filter traffic on a virtual server port. For more information, see access-list command.
- Control management access
- Support source NAT. For more information, see ip nat inside source command.

Example

This example shows how to use an object group in an ACL configuration. This object group defines some static subnets that will be bypasssed in a subsequent ACL configuration:

```
ACOS(config)# object-group network bypass_list
ACOS(config-network:bypass_list)# description Static Subnets
for Bypass
ACOS(config-network:bypass_list)# 192.168.10.10 0.0.0.255
ACOS(config-network:bypass_list)# 192.168.20.10 0.0.0.255
ACOS(config-network:bypass_list)# 192.168.30.10 0.0.0.255
ACOS(config-network:bypass_list)# 192.168.35.10 0.0.0.255
```

Next, configure the ACL using this object group “bypass_list”. Note that no sequence numbers are specified in this example.

```
ACOS(config)# access-list 100 remark "Example ACL"
ACOS(config)# access-list 100 deny ip object-group bypass_list
any
ACOS(config)# access-list 100 permit ip 192.0.0.0
0.255.255.255 any
```

In the `show access-list` command below, note that the ACL sequence numbers have been generated. These sequence numbers are persistent once you perform a write-mem of the configuration.

```
ACOS(config)# show access-list
access-list 100 4 remark “Example ACL”
access-list 100 8 deny ip object-group bypass-list any Data
plane hits: 0
```

```
access-list 100 12 permit ip 172.0.0.0 0.255.255.255 any Data
plane hits: 0
```

ACL statements with object groups are not re-sequenced; if additional ACL statements are added, the `deny` statement containing the object group will always remain immediately above the `permit ip 192.0.0.0` statement.

Related Commands:

- object-group service

accounting

Description Configure TACACS+ as the accounting method for recording information about user activities. The ACOS device supports the following types of accounting:

- EXEC accounting – provides information about EXEC terminal sessions (user shells) on the ACOS device.
- Command accounting – provides information about the EXEC shell commands executed under a specified privilege level. This command also allows you to specify the debug level.

Syntax

```
[no] accounting exec {start-stop | stop-only} {radius | tacplus}
[no] accounting commands cmd-level stop-only tacplus
[no] accounting debug debug-level
```

Parameter	Description
start-stop	Sends an Accounting START packet to TACACS+ servers when a user establishes a CLI session, and an Accounting STOP packet when the user logs out or the session times out.
stop-only	Only sends an Accounting STOP packet when the user logs out or the session times out.
radius | **tacplus**	Specifies the type of accounting server to use.
cmd-level	Specifies which level of commands will be accounted:

Parameter	Description
	• 15 (admin) - commands available to the admin (all commands). • 14 (config) - commands available in config mode (not including the commands of the admin and those under the admin mode). • 1 (priv EXEC) - commands available in privileged EXEC mode. • 0 (user EXEC) - commands available in user EXEC mode. Command levels 2-13 as the same as command level 1.
debug-level	Specifies the debug level for accounting. The debug level is set as flag bits for different types of debug messages. The ACOS device has the following types of debug messages: • 0x1 - Common information such as “trying to connect with TACACS+ servers”, “getting response from TACACS+ servers”; they are recorded in syslog. • 0x2 - Packet fields sent out and received by ACOS, not including the length fields; they are printed out on the terminal. • 0x4 - Length fields of the TACACS+ packets will also be printed on the terminal. • 0x8 - Information about the TACACS+ MD5 encryption is recorded in syslog.

Default N/A

Mode Configuration mode

Usage Available in the shared partition. The accounting server also must be configured.

Example The following command configures the ACOS device to send an Accounting START packet to the previously defined TACACS+ servers

when a user establishes a CLI session on the device. The ACOS device also will send an Accounting STOP packet when a user logs out or their session times out.

```
ACOS(config)# accounting exec start-stop tacplus
```

Example The following command configures the ACOS device to send an Accounting STOP packet when a user logs out or a session times out.

```
ACOS(config)# accounting exec stop-only tacplus
```

Example The following command configures the ACOS device to send an Accounting STOP packet to TACACS+ servers before a CLI command of level 14 is executed.

```
ACOS(config)# accounting commands 14 stop-only tacplus
```

Example The following command specifies debug level 15 for accounting.

```
ACOS(config)# accounting debug 15
```

Related Commands:

- radius-server
- tacacs-server host

acos-events

Description Configures ACOS event-based logging.

Syntax

```
acos-events options
```

Parameter	Description
`active-template` *name*	Configures the name of the global logging template.
`collector-group` *name* `{udp | tcp}`	Configures the name of the log servers group. Options are: • `udp` – Uses UDP syslog protocol to send messages to the log collector. • `tcp` – Uses TCP syslog protocol to send

Parameter	Description
	messages to the log collector
`local-logging`	• `enable` - Enables local-loggingfeature, by default it is disabled. • `rate-limit` - Sets the rate-limit from 1-60000, by default it is 1000. • `max-disk-space` - Sets the maximum disk space from 50-20000 MB, by default it is 100 MB. • `delete-old-logs-in-disk`- Deletes all old logs from the disk.
`log-para-meterization`	Configures Harmony controller log para-meters.
`log-properties`	Configures Logging related properties: • `add-msgid-in-header` - Adds msgid (Message ID) in Syslog messages. This msgid helps to identify the type of message that are filtered on a relay or collector. The msgid is an optional header in syslog. When `add-msgid-in-header` event is set: ◦ The msg-id is added as a part of the header after module name and before the partition name (if any) for Syslog. ◦ Only the msg-id is shown for CEF and not the signature. The 'Trigger-reason' field is used instead of the 'Description' field. • `enable-8K-tcp-syslog` - Enables 8K size remote TCP syslog. • `enable-millisec` - Enables the inclusion

Parameter	Description
	of milliseconds in the log timestamp. The timestamp can have a delay of up to 8 milliseconds. • **NOTE:** The `ClientTimestampFormat` template must be configured in the Syslog server and added to the path of the syslog file to capture the raw syslog messages from the ACOS device. • `use-iso8601-timestamp` - Sends the Syslog messages with the standard header format that includes the year in the timestamp. This is specific only to syslog messages. The timestamp is in the ISO 8601 format (yyyy-mm-ddThh:mm:ss+-ZONE).
`log-server` *name*	Name of the ACOS logging server.
`logdb`	Configures the global logging template with the following options to send logging data to the on-box database. This will cause the data to appear in the GUI logging charts. **NOTE:** You must enable the option for the respective module or there will be no data in the GUI charts. • `enable-all` – Enables logging for all widgets. • `enable-cgn` – Enables CGN logging. • `enable-fw` – Enables Firewall logging. • `enable-http-forward-proxy` – Enables HTTP forward proxy logging.

Parameter	Description
	• `enable-smtp` – Enables SMTP logging. • `enable-ssli` – Enables SSLi logging. Use the enable-fw command to view the GUI charts for firewall logging, as opposed to logs for SSLi data. It is not required to enable SSLi logging for the firewall page.
`message-id` *`name`*	Configures the name of the log message. The *`name`* should specify log message-id lineage.
`message-selector` *`name`*	Configures the message selector to select messages to be logged/blocked. Options include: • `rule` – Configures rules to select messages for which logging is enabled/blocked. Specify a rule index from 1-256, where rules are applied in numeric order. This drops you to another config level, where the following options are available: • `message-id` *`name`* – Selects a specific message by message-id and optionally severity. The following options are available: - **`all`** – Log messages at this level and all sub-trees - **`node-only`** – Log messages at this node only - **`children-only`** – Log messages at all sub-trees only - **`log-field-only`** – Log message for this Log Field only • `severity` – Selects messages with a range of severity values - alert is most severe • `send` – log messages selected by this rule

Parameter	Description
	will be sent • `drop` – log messages selected by this rule will be dropped.
`rate-limit-local`	Configures Rate Limit for local logs.
`rate-limit-remote`	Configures rate limit for logs sent to remote via classic logging configuration.
`statistics [sampling-enable]`	ACOS events global statistics.
`template` *name* `message-selector ms-`*name* `collector-group` *col-name*	Configures the logging template. Options include: • `message-selector` – Specifies the message selector.
`use-partition`	Configures partition for logging.

Default N/A

Mode Configuration mode

Example The following example shows the usage of the **`acos-events`** command:

```
ACOS(config)#acos-events message-selector MS1
ACOS(config-msg-selector:MS1)#rule 1
ACOS(config-msg-selector:MS1-rule:1)#message-id fw all
ACOS(config-msg-selector:MS1-rule:1)#exit
ACOS(config)#acos-events log-server SYSLOG1 20.20.20.20
ACOS(config-log-server)#health-check-disable
ACOS(config-log-server)#port 514 udp
ACOS(config-log-server-logging port)#health-check-disable
ACOS(config-log-server-logging port)#exit
ACOS(config)#acos-events collector-group CG-ASC udp
ACOS(config-collector-group:CG-ASC)#log-server SYSLOG1 514
ACOS(config-collector-group:CG-ASC)#exit
ACOS(config)#acos-events collector-group CG-CEF udp
ACOS(config-collector-group:CG-CEF)#log-server SYSLOG1 514
ACOS(config-collector-group:CG-CEF)#format cef
```

```
ACOS(config-collector-group:CG-CEF)#exit
ACOS(config)#acos-events template FWLOG-ASC
ACOS(config-template:FWLOG-ASC)#message-selector MS1
collector-group CG-ASC
ACOS(config-template:FWLOG-ASC)#exit
ACOS(config)#acos-events template FWLOG-CEF
ACOS(config-template:FWLOG-CEF)#message-selector MS1
collector-group CG-CEF
ACOS(config-template:FWLOG-CEF)#exit
ACOS(config)#acos-events local-logging
ACOS(config-local-log)#rate-limit 20
ACOS(config-local-log)#max-disk-space 150
ACOS(config-local-log)#enable
ACOS(config-local-log)#delete-old-logs-in-disk
ACOS(config-local-log)#exit
ACOS(config)#acos-events log-properties add-msgid-in-header
ACOS(config)#acos-events log-properties enable-8K-tcp-syslog
```

Example The following command enables the inclusion of milliseconds in the timestamp of the logs:

```
ACOS(config)#acos-events log-properties enable-millisec
```

Example The following command uses the standard header format for timestamp which includes milliseconds (if enabled) and the year in the logs (only specific to syslogs):

```
ACOS(config)#acos-events log-properties use-iso8601-timestamp
```

acos-events active-template

Description Configure a global logging template. Only one active template may be specified at a time.

Syntax

```
[no] acos-events active-template name
```

Specify the *name* of an existing logging template, created with the acos-events template command.

Default None.

Mode Global configuration

Example The following example designates LOGTEMP1 as the active logging template:

```
ACOS(config)# acos-events active-template LOGTEMP1
```

acos-events collector-group

Description Configure a group of logging servers. Each logging server is configured with the acos-events log-server command.

Syntax

```
[no] acos-events collector-group name protocol
```

Parameter	Description
name	Name of the collector group of log servers (1-127 characters).
protocol	Specify the syslog protocol to use when sending message to the log collector: tcp udp

This command changes the CLI configuration level where the following additional commands are available:

Command	Description
format	Specify the log message format. You can configure multiple log formats under a collector group. The logs server collects the data in the following format order: • *SYSLOG*: Log message format is syslog. This is the default format. • *CEF*: Log message format is cef. • *LEEF*: Log message format is leef.
health-check *name*	Specify a health check to apply to all log servers in the collector group. Health checks can be configured using the health monitor command.

Command	Description
	If you specify a health check under acos-events log-server it will take precedence over the health check specified here.
`log-dis-tribution`	Configure a log-distribution method. The options are: • *round-robin*: log server selection is based on round-robin. This is the default distribution method. • *hashing*: log messages at the specified node.
`log-server` *name port*	Configure the members (log server name and port) of the collector group.
`rate-limit` *num* `per` *seconds*	Apply a rate-limiter to the collector group. *num* - Maximum number of message allowed per interval (0-2147483647). *seconds* - Interval of time for *num* in seconds (1-100).
`sampling-enable`	Enable baselining.
`server-dis-tribution-hash`	Configure hashing key.

Mode Global configuration

Limitation Even when multiple formats are configured in the collector group, only one format is sent to the log server at a time and the same is displayed in the **`show log`**. For example, if you configure both CEF and SYSLOG formats, the SYSLOG format is sent to the log server. Whereas, if you configure only CEF, then only the CEF format is sent to log server.

Example Below is an example collector group configuration:

```
ACOS(config)# acos-events collector-group CG1 tcp
ACOS(config-collector-group:CG1)# log-server LOG1 115
ACOS(config-collector-group:CG1)# log-server LOG1 125
ACOS(config-collector-group:CG1)# log-server LOG2 115
```

```
ACOS(config-collector-group:CG1)# log-server LOG2 125
ACOS(config-collector-group:CG1)# health-check HEALTH-MON1
```

acos-events log-server

Description Configure a remote logging server.

Syntax

```
[no] acos-events log-server name [ipv4addr | ipv6addr | hostname]
```

Specify one of the following when configuring a new log server; these options can be omitted when editing an existing log server.

Parameter	Description
name	Log server name (1-127 characters).
ipv4addr	Specify the IPv4 address of the remote server.
ipv6addr	Specify the IPv6 address of the remote server.
hostname	Specify the host name of the remote server (1-63 characters).

This command change the CLI level where the following commands are available to enable a health check to be bound to the log server:

Command	Description
`[no] health-check`	Bind a configured health check to the log server. A health check can be configured using the health monitor command.
`[no] health-check-disable`	Disable any health check configured with the log server.
`[no] port` *number* *protocol*	Specify a port *number* (1-65535) and *protocol* (`tcp` or `udp`) to be used for the health checks.

Mode Global configuration

Example Specify a health check and port to be used with log server LOGSRV1:

```
ACOS(config)# acos-events log-server LOGSRV1
```

```
ACOS(config-log-server)# health-check HC1
ACOS(config-log-server)# port 80 tcp
```

acos-events message-id

Description Modify the severity of the specified log messages.

Syntax

```
[no] acos-events message-id lineage
```

Lineage	Description
interface.ethernet.port-state	State of the Ethernet ports.
interface.lif.state	State of the Logical interfaces (LIF).
interface.loopback.port-state	State of the Loopback port.
interface.management.port-state	State of the Management port.
interface.trunk.state	State of the trunk interfaces.
interface.tunnel.intf-state	State of the tunnel interfaces.
interface.ve.state	State of the VE interfaces.
reload.system-state	State of the system reload.

This command changes the CLI configuration level, where the following command is available:

```
[no] property severity severity
```

Parameter	Description
emergency	System unusable log messages (severity=0)
alert	Action must be taken immediately (severity=1)
critical	Critical conditions (severity=2)
error	Error conditions (severity=3)
warning	Warning conditions (severity=4)

Parameter	Description
notification	Normal but significant conditions (severity=5)
information	Informational messages (severity=6)
debugging	Debug level messages (severity=7)

This command is used to change the severity of the log message whose lineage is specified. See the example below.

This command changes the CLI configuration level, where the following command is available:

```
[no] property log-route log route
```

Parameter	Description
local-only	Logs must be sent to local-only (show logging).
remote-only	Logs must be sent to external log servers.
local-and-remote	Logs must be sent to both local and external log servers.

This command is used to change the route of the log message whose lineage is specified. See the example below.

Mode Global configuration mode

Example The following command enters acos-events message-id mode for the Ethernet interface port state and changes the severity messages to critical:

```
ACOS(config)# acos-events message-id interface.ethernet.port-state
ACOS(config-log-msg:interface.ethern)# property severity critical
```

Example The following command enters acos-events message-id mode for the VE interfaces state and specifies that the log messages are to be sent to external log servers:

```
ACOS(config)# acos-events message-id interface.ve.state
ACOS(config-log-msg:interface.ve.sta)# property log-route remote-only
```

acos-events message-selector

Description Configure a message selector to determine which message should be logged or blocked.

Syntax

```
[no] acos-events message-selector name
```

Specify a message selector name (1-63 characters).

This command changes the CLI to a new configuration level, where the following command is available:

```
[no] rule index-num
```

This command creates a rule, used to select or filter log messages as desired. Multiple rules can be configured (up to 255) and they are applied in numerical order; for example, rule 3 would be applied before rule 5.

To create a rule, use the following commands, available after entering the `rule` command:

Command	Description
`message-id` *lineage* [*level*] [*severity*]	Specify a specific message or family of messages to match by this rule. *lineage* - See acos-events message-id for a complete description about lineage. *level* - Specify one of the following: `all` - Match on all messages at the specified lineage level and all lower levels. `node-only` - Match on all messages at the specific lineage level only. `children-only` - Do not match any messages at the specified lineage level, but match all messages at all lower levels. *severity* - See `severity` below for a complete description of the severity options.

Command	Description
`send`	Send log messages that are matched by this rule.
`drop`	Drop log messages that are matched by this rule.
`severity {equal | equal-and-higher} severity-level`	Specify a severity-level of message to match using this rule. Use equal to match only messages of the specified severity. Use equal-and-higher to match messages of the specified severity and all messages of a high severity. For example: `severity equal warning` - matches only log messages that have a level 4 (Warning) severity. `severity equal-and-higher warning` - matches all Warning-level messages, and also all Error, Critical, Alert, and Emergency level messages.

Mode Global configuration

Example Below is an example rule; Ethernet interface log messages equal or more severe than Warning will be sent.

```
ACOS(config)# acos-events message-selector MS1
ACOS(config-msg-selector:MS1)# rule 2
ACOS(config-msg-selector:MS1-rule:2)# message-id
interface.ethernet level all
ACOS(config-msg-selector:MS1-rule:2)# severity equal-and-
higher warning
ACOS(config-msg-selector:MS1-rule:2)# send
```

Related Commands:

- acos-events message-id

acos-events template

Description Configure a global logging template.

You can use the acos-events active-template command to designate a template as the global active logging template.

Syntax

```
[no] acos-events template name
```

Specify a *name* for the template (1-63 characters).

This command changes the CLI configuration level, where the following command is available:

```
[no] message-selector name collector-group name
```

A message selector can be configured using acos-events message-selector. A collector group can be configured using acos-events collector-group.

Mode Global configuration

Example Create a logging template, using MS1 as the message selector and CG1 as the collector group. The configurations for MS1 and CG1 are not shown here.

```
ACOS(config)# acos-events template TEMP1
ACOS(config-template:TEMP1)# message-selector MS1 collector-group CG1
```

admin

Description Configures an admin account for management access to the ACOS device.

Syntax

```
[no] admin admin-username password
```

Command	Description
admin-username	Specifies the system admin user name. User name string (1-31) characters.
password	Specifies the system admin password with prompt. Password string (1-63) characters. The character range is platform-specific. Passwords are case sensitive and can contain special characters. (For more information, see Adding Special Character in Strings.) The default “admin” account password is “a10”.

This command changes the CLI to the configuration level for the specified admin account, where the following admin-related commands are available:

Command	Description
access {cli | web | axapi}	Specifies the use interfaces through which the admin is allowed to access the ACOS device. By default, access is allowed through all user interfaces (CLI, GUI, and aXAPI). For more information, see Supported Access Configuration Commands for Admin Accounts.
cloud-cred	Configures the cloud credentials for the specified cloud-provider. For more information, see admin cloud-cred command.
disable	Disables the admin account. By default, admin accounts are enabled when they are added.
enable	Enables the admin account. By default, admin accounts are enabled when they are added.
password	Specifies the system admin password.
privilege *level*	Sets the privilege *level* for the account: • read – The admin can access the User EXEC and Privileged EXEC levels of the CLI only. • write – The admin can access all levels of the CLI, limited only by a restriction on commands that instantiate or modify the content of external health monitor scripts. • hm – Removes the restriction on the write parameter, which enables admin access to commands that import, create, edit, and delete external health monitor scripts. By default, this privilege is only enabled for the ACOS root admin. The health-external commands that create, edit, and

Command	Description
	delete these scripts are described in the *Command Line Reference for ADC.* Importing these scripts is described in the import command description (import). In ACOS, these monitoring scripts have broad and intimate access throughout the system. Malicious code or content in these scripts could compromise the confidentially, integrity, and availability of the ACOS system and local network infrastructures. It is important to the security of the ACOS system and deployment environment that only admins of sufficient trust be assigned this privilege. It is also the obligation of the ACOS system's administration to make and manage these assignments in securing their deployment of ACOS systems. For more information, see *Application Delivery and Server Load Balancing Guide* (Using *External Health Methods* section) and the *Management Access and Security Guide.* • `partition-read` – The admin has read-only privileges within the L3V partition to which the admin is assigned, and read-only privileges for the shared partition. • `partition-write` – The admin has read-write privileges within the L3V partition to which the admin is assigned. The admin has read-only privileges for the shared partition. • `partition-enable-disable` – The admin has read-only privileges for real servers, with permission to view service port statistics and to disable or re-enable the servers and their service ports. No other read-only or read-write privileges are granted.

Command	Description
	• *partition-name* – The name of the L3V partition to which the admin is assigned. This option applies only to admins that have privilege level `partition-read`, `partition-write`, or `partition-enable-disable`. **NOTE:** L3V partitions are used in Application Delivery Partitioning (ADP). For more information, see *Configuring Application Delivery Partitions* guide. The default privilege is read.
ssh-pubkey *options*	Manage public key authentication for the admin. The `options` are as follows and described in the following rows: • `import` • `delete` • `list`
ssh-pub-keyimport *url*	Imports an authorized public key onto the ACOS device. The *url* specifies the file transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]`

Command	Description
	To enter the entire URL: • `tftp://host/file` • `ftp://[user@]host[port:]/file` • `scp://[user@]host/file` • `sftp://[user@]host/file`
ssh-pub-key delete *num*	Deletes an authorized public key. The *num* specifies the key number on the ACOS device. The key numbers are displayed along with the keys themselves by the `ssh-pubkey list` command. This command can also be used to verify installation of the public key.
ssh-pub-keylist	Lists all the authorized public keys.
trusted-host { ipaddr/*mask-length* | **ipaddr** *subnet-mask* | **access-list** *acl-id* }	Specified the subnet address from which the admin will be allowed access to the ACOS device. You can specify a specific subnet (mask or length) or use a series of hosts configured in an access control list (ACL). The default trusted host is 0.0.0.0/0, which allows access from any host or subnet.
unlock	Unlocks the account. Use this option if the admin has been locked out due to too many login attempts with an incorrect password. The admin-lockout is used to configure lockout parameters.

The following table lists the types of user interface access available for admin accounts.

Table 10 : Supported Access Configuration Commands for Admin Accounts

Command	Access	Result
`access cli`	Only CLI	Admin can access only CLI. No Web or aXAPI.
`access axapi`	Only aXAPI	Admin can access only aXAPI. No CLI or Web.
`access web`	Only Web (and aXAPI)	Admin can access Web and aXAPI automatically included.
`access cli axapi`	CLI and aXAPI	Admin can access both CLI and aXAPI.
`access cli web`	CLI, Web, and aXAPI	Admin can access CLI, Web, and aXAPI.

NOTE: To restrict user interface access, configure only the necessary access modes. For example, if you want to restrict aXAPI access, provide access to CLI only by using access `cli` command.

Default The system has a default admin account, with username “admin” and password “a10”. The default admin account has write privilege and can log on from any host or subnet address.

Other defaults are described in the descriptions above.

Mode Configuration mode

Usage An additional session is reserved for the “admin” account to ensure access. If the maximum number of concurrent open sessions is reached, the “admin” admin can still log in using the reserved session. This reserved session is available only to the “admin” account.

Example The following command inputs the admin user password:

```
ACOS(config)# admin adminuser1 password
Password:
Retype password:
Modify Admin User successful!
ACOS(config-admin:adminuser1)#
```

NOTE: The password is obfuscated and therefore it is not displayed on the screen.

Example The following commands add admin “adminuser1” with password using `password` sub-command:

```
ACOS(config)# admin adminuser1
ACOS(config-admin:adminuser1)# password
Password:
Retype password:
ACOS(config-admin:adminuser1)#
```

NOTE: The password is obfuscated and therefore it is not displayed on the screen.

Example The following commands add admin “adminuser2” with write privilege, and restrict login access to the 10.10.10.x subnet only:

```
ACOS(config)# admin adminuser2 password
Password:
Retype password:
Modify Admin User successful!
ACOS(config-admin:adminuser2)# privilege write
ACOS(config-admin:adminuser2)# trusted-host10.10.10.0 /24
```

Example The following commands configure an admin account for a private partition:

```
ACOS(config)# admin adminuser2 password
Password:
Retype password:
Modify Admin User successful!
ACOS(config-admin:adminuser2)# privilege partition-write
companyA
Modify Admin User successful !
```

Example The following commands provide CLI and aXAPI access to adminuser2:

```
ACOS(config)# admin adminuser2
ACOS(config-admin:adminuser2)# access cli
ACOS(config-admin:adminuser2)# access axapi
```

Example The following commands add admin “adminuser3” with default privileges, and restricts login access as defined by access list 2. The show output confirms that “ACL 2” is the trusted host:

```
ACOS(config)# admin adminuser3 password
Password:
Retype password:
Modify Admin User successful!
ACOS(config-adminuser3)# trusted-host access-list 2
Modify Admin User successful!
ACOS(config-adminuser3)# show admin adminuser3 detail
  User Name              ...... adminuser3
  Status                 ...... Enabled
  Privilege              ...... R
  Partition              ......
  Access type            ...... cli web axapi
  GUI role               ...... ReadOnlyAdmin
  Trusted Host(Netmask)  ...... ACL 2
  Lock Status            ...... No
  Lock Time              ......
  Unlock Time            ......
```

Related Commands:

- enable-password

admin cloud-cred

Description Configures the cloud credentials for the specified cloud-provider.

Syntax

```
[no] admin admin-username
cloud-cred { aws-cred | aws-config | azure-cred | vmware-cred
 } options
```

Command	Description
admin-username	Specifies the system admin user name. User name string (1-31) characters.

This command changes the CLI to the configuration level for the specified admin account, where the following admin-related command is available:

Command	Description
cloud-cred {**aws-cred** | **aws-config** | **azure-cred** | **vmware-cred**} *options*	Configures the cloud credentials for the specified cloud-provider. The cloud credentials can be provided for the specific cloud platform: • **aws-cred** • **aws-config** • **azure-cred** • **vmware-cred** The *options* for each cloud credentials configuration are as follows and described in the following rows: • **import** • **delete** • **show**
import *[use-mgmt-port] url*	Imports the AWS, Azure, or VMware credentials file or AWS configuration file on the ACOS device. • *use-mgmt-port* - Specifies the management port as the source port. • *url* - Specifies the file transfer protocol, username (if required), and directory path. You can enter the complete URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the complete URL, you will still be prompted for a password. The password can be up to 255 characters in length and supports the following special

Command	Description
	characters too: `!#$()*+,-.;=^_`{|}~` The following special characters are not supported: `(blank space) "%&'/:<>?@[\]` To enter the complete URL: • `tftp://host/file` • `ftp://[user@]host[port:]/file` • `scp://[user@]host/file` • `sftp://[user@]host/file`
delete	Deletes the AWS, Azure, or VMware credentials file or AWS configuration file from the ACOS device.
show	Shows the AWS, Azure, or VMware credentials file or AWS configuration file configuration on the ACOS device.

Mode Privileged EXEC

Usage The cloud `credentials` file must be imported to the cloud platform where the vThunder instance is running. For enabling vThunder ADC logs and metrics on AWS, Azure, and VMware, see the respective *vThunder Installation Guides*.

Limitation The Internal Thunder Observability Agent (iTOA) and High Availability (HA) uses the same cloud credentials. The location and filename of the Cloud Credentials Import files and HA credentials files for AWS and Azure are the same. So, if the HA is already configured for AWS or Azure, the new **cloud-cred** import files override the existing HA credentials file. Similarly, if cloud credentials for iTOA is already configured, the new HA credentials file overrides the existing **cloud-cred** import file.

The following files have the same location for HA and Cloud Credentials Import:

- /a10data/.aws/config
- /a10data/.aws/credentials
- /a10data/.azure/credentials

Example The following commands import the AWS credentials on an ACOS device:

```
ACOS(config)# admin adminuser2
ACOS(config-admin:adminuser2)# cloud-cred aws-cred import
tftp://192.168.0.0/credentials.txt
```

Example The following command shows the imported AWS credentials file information:

```
ACOS(config-admin:adminuser2)# cloud-cred aws-cred show
[default]
aws_access_key_id = XXXX
aws_secret_access_key = XXXX
```

Related Commands:

- cloud-services cloud-provider

admin-lockout

Description Set lockout parameters for admin sessions.

Syntax

```
[no] admin-lockout
{duration minutes | enable | reset-time minutes | threshold
number}
```

Parameter	Description
duration *minutes*	Number of minutes a lockout remains in effect. After the lockout times out, the admin can try again to log in. You can specify 0-1440 minutes. To keep accounts locked until you or another authorized administrator unlocks them, specify 0. The default duration is 10 minutes.

Parameter	Description
enable	Enables the admin lockout feature. The lockout feature is disabled by default.
reset-time *minutes*	Number of minutes the ACOS device remembers failed login attempts. You can specify 1-1440 minutes. The default reset time is 10 minutes.
threshold *number*	Number of consecutive failed login attempts allowed before an administrator is locked out. You can specify 1-10. The default threshold is 5.

Example The following command enables admin lockout:

```
ACOS(config)# admin-lockout enable
```

admin-session clear

Description Terminate admin sessions.

Syntax

```
admin-session clear {all | session-id}
```

Parameter	Description
all	Clears all other admin sessions with the ACOS device except yours.
session-id	Clears only the admin session you specify. To display a list of active admin sessions, including their session IDs, use show admin command.

Default N/A

Mode Configuration mode

aflex

Description Configure and manage aFleX policies.

For more information, see *aFleX Scripting Language Reference Guide*.

Syntax

```
aflex {
check name |
copy src-name dst-name |
create name |
delete name |
help |
rename src-name dst-name
}
```

Parameter	Description
check	Check the syntax of the specified aFleX script.
copy	Copy the *src-name* aFleX script to *dst-name*.
create	Create an aFleX script with the specified *name*.
delete	Delete the specified aFleX script.
help	View aFleX help.
rename	Rename an aFleX script from *src-name* to *dst-name*.

Mode Global configuration mode

aflex-scripts start

Description Begin a transaction to edit an aFleX script within the CLI.

For more information, see*aFleX Scripting Language Reference Guide*.

Syntax

```
aflex-script start
```

Mode Global configuration mode

arp

Description Create a static ARP entry.

Syntax

```
[no] arp ipaddr mac-address
[interface {ethernet port-num | trunk trunk-id} [vlan vlan-
id]]
```

Parameter	Description
ipaddr	IP address of the static entry.

Parameter	Description
mac-address	MAC address of the static entry.
port-num	Ethernet port number.
trunk-id	Trunk ID number.
vlan-id	If the ACOS device is deployed in transparent mode, and the interface is a tagged member of multiple VLANs, use this option to specify the VLAN for which to add the ARP entry.

Default The default timeout for learned entries is 300 seconds. Static entries do not time out.

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

arp-timeout

Description Change the aging timer for dynamic ARP entries.

Syntax

```
[no] arp-timeout seconds
```

Replace *seconds* with the number of seconds a dynamic entry can remain unused before being removed from the ARP table (60-86400).

Default 300 seconds (5 minutes)

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

audit

Description Configure command auditing.

Syntax

```
[no] audit {enable [privilege] | size num-entries}
```

Parameter	Description
enable	Enables command auditing. Command auditing is enabled by default.
privilege	Enables logging of Privileged EXEC commands. Without this option, only configuration commands are logged.
num-entries	Specifies the number of entries the audit log file can hold. You can specify 1000-30000 entries. When the log is full, the oldest entries are removed to make room for new entries. When the feature is enabled, the audit log can hold 20,000 entries by default.

Mode Configuration mode

Usage Command auditing logs the following types of system management events:

- Admin login and logout operations for CLI, GUI, and aXAPI sessions
- Unsuccessful admin login attempts
- Configuration changes. All attempts to change the configuration are logged, even if they are unsuccessful.
- CLI commands at the Privileged EXEC level (if audit logging is enabled for this level)

The audit log is maintained in a separate file, apart from the system log. The audit log is ADP-aware. The audit log messages that are displayed for an admin depend upon the admin's role (privilege level). Admins with Root, Read Write, or Read Only privileges who view the audit log can view all the messages, for all system partitions.

Admins who have privileges only within a specific partition can view only the audit log messages related to management of that partition. Partition Read-Only admins can not view any audit log entries.

For more information, see "Command Auditing" chapter of the *Management Access and Security Guide*

NOTE: Backups of the system log include the audit log.

Disabling Command Audit Logging

Use `no audit enable` to disable command audit logging. Note that this command is not saved to the running configuration, and therefore does not persist across system reload and reboot operations.

authentication console type

Description Configure a console authentication type.

Syntax

```
[no] authentication console type {ldap | local | radius | tacplus}
```

Parameter	Description
ldap	Use LDAP for console authentication
local	Use the ACOS configuration for console authentication.
radius	Use RADIUS for console authentication.
tacplus	Use TACACS+ for console authentication.

Mode Configuration mode

Usage Available in the shared partition. You can specify as many options as needed. For more information, see "TACACS+ and RADIUS" chapter of the *Management Access and Security Guide*.

Example The following example grants LDAP and local console authentication:

```
ACOS(config)# authentication console type ldap local
```

authentication enable

Description Configuration authentication of admin enable (Privileged mode) access.

Syntax

```
[no] authentication enable {local [tacplus] | tacplus [local]}
```

Parameter	Description
`local`	Uses the ACOS configuration for authentication of the enable password.
`tacplus`	Uses TACACS+ for authentication of the enable password.

Default local

Mode Configuration mode

Usage Available in the shared partition. The **`authentication enable`** command operates differently depending on the **`authentication mode`** command setting:

- For **`authentication mode multiple`**, the ACOS device will attempt to authenticate the admin with the first specified method. If the first method fails, the next specified method is used.
- For **`authentication mode single`**, the ACOS device will attempt to authenticate the admin with the first specified method. If the method fails, the ACOS device will return an error. By default, **`authentication mode single`** is selected.

Related Commands:

- authentication mode

authentication login privilege-mode

Description Places TACACS+-authenticated admins who log into the CLI at the Privileged EXEC level of the CLI instead of at the User EXEC level.

Syntax

```
[no] authentication login privilege-mode
```

Default Disabled

Mode Configuration mode

Usage Available in the shared partition.

authentication mode

Description Enable tiered authentication.

Syntax

```
[no] authentication mode {multiple | single}
```

Parameter	Description
multiple	Enable "tiered" authentication, where the ACOS device will check the next method even if the primary method does respond but authentication fails using that method. For example, if the primary method is RADIUS and the next method is TACACS+, and RADIUS rejects the admin, tiered authentication attempts to authenticate the admin using TACACS+. This authentication behavior is summarized below: • Try *method1*. If a *method1* server replies, permit or deny access based on the server reply. • If no *method1* servers reply *or* a *method1* server denies access, try *method2*. • If no *method2* servers reply *or* a *method2* server denies access, try *method3*. • If no *method3* servers reply *or* a *method3* server denies access, try *method4*. If authentication succeeds, the admin is permitted. Otherwise, the admin is denied.
single	Enable single authentication mode, where the backup authentication method will only be used if the primary method does not respond. If the primary method *does* respond but denies access, then the secondary method is simply not used. The admin is not granted access. This authentication behavior is summarized below: • Try *method1*. If a *method1* server replies, permit or deny access based on the server reply. • *Only* if no *method1* servers reply, try method2. If a *method2* server replies, permit or deny access based

Parameter	Description
	on the server reply • *Only* if no *method2* servers reply, try method3. If a *method3* server replies, permit or deny access based on the server reply. • *Only* if no *method3* servers reply, try *method4*. If authentication succeeds, the admin is permitted. Otherwise, the admin is denied.

Default By default, **single** authentication mode is used.

Mode Configuration mode

Usage Available in the shared partition

authentication multiple-auth-reject

Description Do not allow multiple concurrent admin sessions using the same account.

Syntax

```
[no] authentication multiple-auth-reject
```

Default Disabled. Multiple concurrent admin sessions using the same account are allowed.

Mode Global configuration

Usage Available in the shared partition

authentication type

Description Set the authentication method used to authenticate administrative access to the ACOS device.

Syntax

```
[no] authentication [console] type  method1
[method2 [method3 [method4]]]
```

Parameter	Description
console	Applies the authentication settings only to access through the console (serial) port. Without this

Parameter	Description
	option, the settings apply to all types of admin access.
type *method1* [*method2* [*method3* [*method4*]]]	Uses the ACOS configuration for authentication. If the administrative username and password match an entry in the configuration, the administrator is granted access. The following authentication types are supported: • **ldap**–Uses an external LDAP server for authentication. • **local**–Uses the ACOS configuration for authentication. If the administrative username and password match an entry in the configuration, the administrator is granted access. • **radius**–Uses an external RADIUS server for authentication. • **tacplus**–Uses an external TACACS+ server for authentication. By default, only local authentication is used.

Default By default, only local authentication is used.

Mode Configuration mode

Usage Available in the shared partition. The local database (**local** option) must be included as one of the authentication sources, regardless of the order is which the sources are used. Authentication using only a remote server is not supported.

Example The following commands configure a pair of RADIUS servers and configure the ACOS device to try them first, before using the local database. Since 10.10.10.12 is added first, this server will be used as the primary server. Server 10.10.10.13 will be used only if the primary server is unavailable. The local database will be used only if both RADIUS servers are unavailable.

```
ACOS(config)# radius-server host 10.10.10.12 secret radp1
ACOS(config)# radius-server host 10.10.10.13 secret radp2
ACOS(config)# authentication type radius local
```

Related Commands:

- radius-server
- tacacs-server host

authorization

Description Configure authorization for controlling access to functions in the CLI. The ACOS device can use TACACS+ for authorizing commands executed under a specified privilege level. This command also allows the user to specify the level for authorization debugging.

Syntax

```
[no] authorization commands cmd-level method {tacplus [none] | none}

[no] authorization debug debug-level
```

Parameter	Description
commands *cmd-level* ***method***	Specifies the level of commands that will be authorized. The commands are divided into the following levels: • Privilege 0: Read-only • Privilege 1: Read-write • Privilege 2–4: Not-used • Privilege 5–14: Reserved for ACOS-specific roles • Privilege 15: Read-write
tacplus	Specifies TACACS+ as the authorization method. (If you omit this option, you must specify none as the method, in which case no authorization will be performed.)
tacplus **none**	If all the TACACS+ servers fail to respond, then no further authorization will be performed and the command is allowed to execute.

Parameter	Description
none	No authorization will be performed.
debug *debug-level*	Specifies the debug level for authorization. The debug level is set as flag bits for different types of debug messages. The ACOS device has the following types of debug messages: • 0x1 – Common system events such as “trying to connect with TACACS+ servers” and “getting response from TACACS+ servers”. These events are recorded in the syslog. • 0x2 – Packet fields sent out and received by the ACOS device, not including the length fields. These events are written to the terminal. • 0x4 – Length fields of the TACACS+ packets will also be displayed on the terminal. • 0x8 – Information about TACACS+ MD5 encryption will be sent to the syslog.

Default Not set

Mode Configuration mode

Usage Available in the shared partition. The authorization server also must be configured.

Example The following command specifies the authorization method for commands executed at level 14: try TACACS+ first but if it fails to respond, then allow the command to execute without authorization.

```
ACOS(config)# authorization commands 14 method tacplus none
```

The following command specifies debug level 15 for authorization:

```
ACOS(config)# authorization debug 15
```

Related Commands:

- radius-server
- tacacs-server host

automatic-update

Description For Application aware firewall, configures automatic updates, connecting through the proxy-server, proxy IP address, HTTP port, or management port, with settings for authentication. Configures updates manually with check-now option. Currently only the application firewall feature is supported with this command.

Syntax

```
automatic-update {use-mgmt-port | proxy-server {check-now
|revert} feature_name
```

Parameter	Description
`check-now app-fw`	Manually check for update now.
`proxy-server`	Connect through proxy server.
`use-mgmt-port`	Use management port to connect. By default, ACOS will download the update file through management port.
`auth-type`	Select proxy authentication type (Basic).
`https-port`	Proxy server HTTPS port (HTTP port will be used if not configured).
`password`	Password for proxy authentication.
`proxy-server`	Proxy server hostname or IP address.
`username`	Username for proxy authentication.
`feature-name`	The name of the feature. For example, app_fw - application firewall.
`check-now` *`feature-name`*	Manually upgrade software to the latest version (operational command).
`revert` *`feature-name`*	Manually revert software to previous successfully installed version.
`reset` *`feature-name`*	Manually reset software to default version (operational command - hidden)

Default N/A

Mode Shared configuration mode

Example The following example shows the usage of the **automatic-update** command:

```
ACOS (config)# automatic-update use-mgmt-port
ACOS (config)# automatic-update proxy-server
ACOS (config)# automatic-update check-now app-fw
ACOS (config)# automatic-update revert app-fw
ACOS (config)# automatic-update reset app-fw
```

automatic-update central-cert-pin-list

Description Configure the schedule to update the central certificate pinning candidate list periodically from the GLM server.

Syntax **[no] automatic-update central-cert-pin-list {schedule {daily | weekly}}**

Parameter	Description
daily *{hh:mm}*	Specify the daily time to update the central-cert-pin-list. The time is *hh:mm* 24-hours local time format.
weekly *{Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday}*	Specify the weekly day and time to update the central-cert-pin-list. The week can be specified as: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. The time can be specified as 24-hours local time format: hh:mm

Default Not enabled

Mode Configuration mode

NOTE: If ACOS needs to use the management interface to connect to the GLM server, you need to configure **automatic-update use-mgmt-port**.

Example The following example configures the schedule to automatically update the list daily:

```
ACOS(config)# automatic-update central-cert-pin-list schedule daily 12:30
```

Example The following example stops the task to automatically update the list daily:

```
ACOS(config)# no automatic-update central-cert-pin-list schedule daily
```

Example The following example configures the schedule to automatically update the list on a weekly basis:

```
ACOS(config)# automatic-update central-cert-pin-list schedule weekly Tuesday 12:30
```

automatic-update check-now

Description Immediately update the specified parameter to the latest version from the GLM server.

When the automatic update schedule is triggered on the dual blade Multi-PU platforms, the PU1 and PU2 update and install the bundle files.

Prerequisite Before using **automatic-update** options, make sure that the device is registered with the Global License Manager (GLM). For more information on registering the device, refer *Global License Manager User Guide.*

NOTE: This feature is available for shared partition only.

Syntax

```
[no] automatic-update check-now  [ app-fw | ca-bundle | a10-threat-intel ]
```

Parameter	Description
app-fw	Specify this option to immediately check the application firewall protocol bundle. A valid Qosmos license is required.
ca-bundle	Specify this option to immediately update the ca cert bundle. A valid Thunder license is required.
a10-threat-intel	Specify this option to immediately update the A10 Threat Intel list. A valid A10 Threat Intel license is required.

Default Not enabled

Mode Configuration mode

Example The following example configures automatic-update:

```
ACOS(config)# automatic-update check-now app-fw
ACOS(config)# automatic-update check-now ca-bundle
ACOS(config)# automatic-update check-now a10-threat-intel
```

automatic-update proxy-server

Description Proxy server to update the CA bundle and application firewall protocol bundle from the GLM server.

NOTE: This feature is available for shared partition only.

Syntax

```
automatic-update proxy-server{auth-type | https-port | password | username| proxy-host}
```

Parameter	Description
auth-type{ntlm {domain}| basic}	Select the proxy authentication type as NTLM or Basic. When you set NTML option, then you can configure 'domain' to specify the realm of the

Parameter	Description
	NTML authentication. The value can be alphanumeric and up to 127 characters are allowed.
https-port	Specify the proxy server HTTPS port. The value can be between 1-65535.
proxy-host	Specify the proxy server host name or IP address. The value can be alphanumeric and up to 127 characters are allowed.
username	Specify the username for proxy authentication. The value can be alphanumeric and up to 127 characters are allowed.
password	Specify the password for proxy authentication. The value can be alphanumeric and up to 127 characters are allowed.

Default Not enabled

Mode Configuration mode

Example The following example configures the schedule to automatically update the list daily:

```
ACOS(config)# automatic-updateproxy-server
ACOS(config-proxy-server)# auth-typebasic
ACOS(config-proxy-server)# proxy-host10.1.1.1
ACOS(config-proxy-server)# usernametest
ACOS(config-proxy-server)# passwordtest
```

automatic-update revert

Description Immediately revert to the previous version of the specified parameter.

When the automatic update schedule is triggered on the dual blade Multi-PU platforms, the PU1 and PU2 update and install the bundle files.

NOTE: This feature is available for shared partition only.

Syntax

```
[no] automatic-update revert [ a10-threat-intel | app-fw ]
```

Parameter	Description
a10-threat-intel	The A10 Threat Intel list.
app-fw	The Application Firewall protocol bundle.

Default Not enabled

Mode Configuration mode

Example The following example reverts to the previous version of the A10 Threat Intel list:

```
ACOS(config)# automatic-update revert a10-threat-intel
```

NOTE: The execution will fail if the previous version of the A10 Threat Intel list does not exist.

automatic-update app-fw

Description Configure the schedule to update the application firewall protocol bundle latest version from the GLM server.

When the automatic update schedule is triggered on the dual blade Multi-PU platforms, the PU1 and PU2 update and install the bundle files.

NOTE: This feature is available for shared partition only.

Syntax

```
[no]automatic-update app-fw{schedule {daily | weekly}}
```

Parameter	Description
daily{hh:mm}	Specify the daily time to update the application firewall protocol bundle latest version.

Parameter	Description
	The time is *hh:mm* 24-hours local time format.
weekly{Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday}	Specify the weekly day and time to update the application firewall protocol bundle latest version. The week can be specified as: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. The time can be specified as 24-hours local time format.: hh:mm

Default Not enabled

Mode Configuration mode

Example The following example configures the automatic-update schedule:

```
ACOS(config)# automatic-update app-fw scheduledaily 12:30
```

automatic-update ca-bundle

Description Configure the schedule to update the CA bundle version from the GLM server.

When the automatic update schedule is triggered on the dual blade Multi-PU platforms, the PU1 and PU2 update and install the bundle files.

NOTE: This feature is available for shared partition only.

Syntax

```
automatic-update ca-bundle{schedule {daily | weekly}}
```

Parameter	Description
daily{hh:mm}	Specify the daily time to update the CA bundle latest version.

Parameter	Description
	The time is *hh:mm* 24-hours local time format.
weekly{Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday}	Specify the weekly day and time to update the CA bundle latest version. The week can be specified as: `Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday`. The time can be specified as 24-hours local time format.: `hh:mm`

Default Not enabled

Mode Configuration mode

Example The following example configures the automatic-update schedule:

```
ACOS(config)# automatic-update ca-bundle schedule daily 12:30
```

automatic-update a10-threat-intel

Description Configure the schedule to update the A10 Threat Intel list from the GLM server.

When the automatic update schedule is triggered on the dual blade Multi-PU platforms, the PU1 and PU2 update and install the bundle files.

For more information on A10 Threat Intel list, refer to the *Firewall Configuration* guide .

NOTE: This feature is available for shared partition only.

Syntax

```
[no] automatic-update a10-threat-intel {schedule {daily | weekly}}
```

Parameter	Description
daily *{hh:mm}*	Specify the daily time to update the A10 Threat Intel list. The time is *hh:mm* 24-hours local time format.
weekly *{Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday}*	Specify the weekly day and time to update the A10 Threat Intel list. The week can be specified as: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. The time can be specified as 24-hours local time format: hh:mm

Default Not enabled

Mode Configuration mode

NOTE: If ACOS needs to use the management interface to connect to the GLM server, you need to configure **automatic-update use-mgmt-port**.

Example The following example configures the schedule to automatically update the A10 Threat Intel list daily:

```
ACOS(config)# automatic-update a10-threat-intel schedule daily 12:30
```

Example The following example stops the task to automatically update the A10 Threat Intel list daily:

```
ACOS(config)# no automatic-update a10-threat-intel schedule daily 12:30
```

Example The following example configures the schedule to automatically update the A10 Threat Intel list on a weekly basis:

```
ACOS(config)# automatic-update a10-threat-intel schedule weekly Tuesday 12:30
```

automatic-update use-mgmt-port

Description Use management port to connect to the GLM server.

NOTE: This feature is available for shared partition only.

Syntax

```
[no] automatic-update use-mgmt-port
```

Default Not enabled

Mode Configuration mode

automatic-update schedule

Description For Application aware firewall, configures the schedule for automatic update

Syntax

```
automatic-update <feature-name> schedule {weekly {Monday | Tuesday | Wednesday| Thursday| Saturday| Sunday} <time> | {daily <time>}}
```

Parameter	Description
feature-name	The name of the feature. For example, app_fw: application firewall.
schedule weekly	Download and install the latest protocol bundles automatically. The options are weekly on a specified day and time. The time format is “HH:MM” in 24-hour local time.
schedule daily	ACOS downloads and installs the latest bundles automatically. The options are weekly on a specified day and time. The time format is “HH:MM” in 24-hour local time.

Mode Global configuration mode

Example

```
ACOS (config)# automatic-update app-fw schedule daily 17:32 ?
```

backup store

Description Configure and save file access information for backup. When you back up system information, you can save typing by specifying the name of the store instead of the options in the store.

Syntax

```
[no] backup store {create store-name url | delete store-name}
```

Parameter	Description
store-name	Name of the store.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]`  To enter the entire URL:  `tftp://host/file`  `ftp://[user@]host[port:]/file`  `scp://[user@]host/file`  `sftp://[user@]host/file`

Default None

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Related Commands:

- restore
- backup log
- backup system
- backup-periodic

backup-periodic

Description Schedule periodic backups.

NOTE: After configuring this feature, make sure to save the configuration. If the device resets before the configuration is saved, the backups will not occur.

Syntax

```
[no] backup-periodic {target [...]}
{hour num | day num | week num}
{[use-mgmt-port] url}
```

Parameter	Description
target	• Specify **system** to back up the following system files: ◦ Startup-config files ◦ Admin accounts and login and enable passwords ◦ aFleX scripts ◦ Class lists and black/white lists ◦ Scripts for external health monitors ◦ SSL certificates, keys, and certificate revocation lists ◦ If custom configuration profiles are mapped to the startup-config, they also are backed up. • Specify **log** to back up the system log.

Parameter	Description
	You can specify either option, or both options.
hour *num* | **day** *num* | **week** *num*	Specifies how often to perform the back ups. You can specify one of the following: • **hour** *num*—Performs the backup each time the specified number of hours passes. For example, specifying **hour 3** causes the backup to occur every 3 hours. You can specify 1-65534 hours. There is no default. • **day** *num*—Performs the backup each time the specified number of days passes. For example, specifying **day 5** causes the backup to occur every 5 days. You can specify 1-199 days. There is no default. • **week** *num*—Performs the backup each time the specified number of weeks passes. For example, specifying **week 4** causes the backup to occur every 4 weeks. You can specify 1-199 weeks. There is no default.
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	Specifies the file transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters:

Parameter	Description
	!#$()*+,-.;=^_`{|}~ The following special characters are not supported: (blank space) "%&'/:<>?@[\] To enter the entire URL: • **tftp://***host***/***file* • **ftp://**[*user***@**]*host*[:*port*]**/***file* • **scp://**[*user***@**]*host***/***file* • **sftp://**[*user***@**]*host***/***file*

Default Not set

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following commands schedule weekly backups of the entire system, verify the configuration, and save the backup schedule to the startup-config:

```
ACOS(config)# backup-periodic system week 1
ftp://admin2@10.10.10.4/weekly-sys-backup
Password []?<characters not shown>
Do you want to save the remote host information to a profile
for later use?[yes/no]yes
Please provide a profile name to store remote url:wksysbackup
ACOS(config)# show backup
backup periodically system week 1
ftp://admin2@10.10.10.4//weekly-sys-backup
Next backup will occur at 14:37:00 PDT Thu Aug 19 2014
ACOS(config)# write memory
Building configuration...
[OK]
```

banner

Description Set the banners to be displayed when an admin logs onto the CLI or accesses the Privileged EXEC mode.

Syntax

```
[no] banner {exec | login} [multi-line end-marker] line
```

Parameter	Description
exec	Configures the EXEC mode banner (1-2048 characters).
login	Configures the login banner (1-2048 characters).
multi-line *end-marker*	Hexadecimal number to indicate the end of a multi-line message. The end marker is a simple string up to 2-characters long, each of the which must be an ASCII character from the following range: 0x21-0x7e. The multi-line banner text starts from the first line and ends at the marker. If the end marker is on a new line by itself, the last line of the banner text will be empty. If you do not want the last line to be empty, put the end marker at the end of the last non-empty line.
line	Specifies the banner text.

Default The default login banner is “ACOS system is ready now.”

The default EXEC banner is “[type ? for help]”.

Mode Configuration mode

Example The following examples set the login banner to “Welcome to Login Mode” and sets the EXEC banner to a multi-line greeting:

```
ACOS(config)# banner login Welcome to Login Mode
ACOS(config)# banner exec multi-line
Input a string to mark the end of banner text, up to 2
characters:
bb
Enter text message, end with string 'bb'.
Welcome to EXEC Mode.
This is the second line of the banner.
```

```
And here is yet another (third) line.
bb
ACOS(config)#
```

bfd echo

Description Enables echo support for Bidirectional Forwarding Detection (BFD).

Syntax

```
[no] bfd echo
```

Default Disabled

Mode Configuration mode

Usage BFD echo enables a device to test data path to the neighbor and back. When a device generates a BFD echo packet, the packet uses the routing link to the neighbor device to reach the device. The neighbor device is expected to send the packet back over the same link.

NOTE:

- On the remote end, BFD and BFD echo modes need to be enabled globally and on the interface.
- The BFD echo packets will be dropped if any of the following commands is configured:
  - `ip anomaly-drop drop-all`
  - `ip anomaly-drop security-attack layer-3`

bfd enable

Description Globally enable BFD packet processing.

Syntax

```
[no] bfd enable
```

Default Disabled

Mode Configuration mode

bfd interval

Description Configure BFD timers.

Syntax

```
[no] bfd interval ms min-rx ms multiplier num
```

Parameter	Description
interval *ms*	Rate at which the ACOS device sends BFD control packets to its BFD neighbors. You can specify 48-1000 milliseconds (ms). The default is 800 ms.
min-rx *ms*	Minimum amount of time in milliseconds that the ACOS device waits to receive a BFD control packet from a BFD neighbor. If a control packet is not received within the specified time, the multiplier (below) is incremented by 1. You can specify 48-1000 ms. The default is 800 ms.
multiplier *num*	Maximum number of consecutive times the ACOS device will wait for a BFD control packet from a neighbor. If the multiplier value is reached, the ACOS device concludes that the routing process on the neighbor is down. You can specify 3-50. The default is 4

Usage If you configure the interval timers on an individual interface, then the interface settings are used instead of the global settings. Similarly, if the BFD timers have not been configured on an interface, then the interface will use the global settings.

NOTE: BFD always uses the globally configured interval timer if it's for a BGP loopback neighbor.

block-abort

Description Use this command to exit block-merge or block-replace mode without implementing the new configurations made in block mode.

Syntax

```
block-abort
```

Default N/A

Mode Block-merge or block-replace configuration mode

Usage Use this command to discard any changes you make while in block-merge or block-replace mode. In order to exit block mode without committing the new configuration changes, use **block-abort**. This command must be entered before `block-merge-end` or `block-replace-end` in order for all block configuration changes to be deleted. This command ends block configuration mode.

block-merge-end

Description Use this command to exit block-merge mode and integrate new configurations into the current running config.

Syntax

```
block-merge-end
```

Default N/A

Mode Block-merge configuration mode

Usage This command exits block-merge configuration mode and merges all of your new configuration with the existing running configuration. In the case of overlapping configurations, the new configuration will be used and any child instances will be deleted. Any old configurations which are not replaced in block-merge mode will remain in the running configuration after this command is entered. The new configurations are merged into the running configuration without disturbing live traffic.

block-merge-start

Description Use this command to enter block-merge configuration mode.

Syntax

```
block-merge-start
```

This command takes you to the Block-merge configuration level, where all configuration commands are available.

Default Disabled.

Mode Global configuration mode.

Usage This command enters block-merge configuration mode but leaves the ACOS device up. While in block-merge mode, new configurations will

not be entered into the running configuration. At the block-merge configuration level, you can enter new configurations which you want to merge into the running configuration. Any configuration that overlaps with the current running configuration will be replaced when ending block-merge mode. Any configurations in the running config which are not configured in block-merge mode will continue to be included in the running configuration mode after exiting block-merge mode.

block-replace-end

Description Enter this command to end block-replace configuration mode and replace the current running configuration with the new configurations.

Syntax

```
block-replace-end
```

Default N/A

Mode Block-replace configuration mode.

Usage This command exits block-replace configuration mode and replaces all of your existing configuration with the new configuration. Any old configurations which are not replaced in block-replace mode will be removed in the running configuration after this command is entered. The new configurations become the running configuration without disturbing live traffic.

block-replace-start

Description Use this command to enter block-replace configuration mode.

Syntax

```
block-replace-start
```

This command takes you to the Block-replace configuration level, where all configuration commands are available.

Default Disabled.

Mode Global configuration mode.

Usage This command enters block-replace configuration mode but leaves the ACOS device up. While in block-replace mode, new configurations will

not be entered into the running configuration. At the block-replace configuration level, you can enter a new configuration which you want to replace the running configuration. All of the running configuration will be replaced when ending block-merge mode. If an object that exists in the running configuration is not configured in block-replace, then all configurations for that object will be removed upon ending block-replace mode.

boot-block-fix

Description Repair the master boot record (MBR) on the hard drive or compact flash.

Syntax

```
boot-block-fix {cf | hd}
```

Parameter	Description
cf	Repair the compact flash.
hd	Repair the hard disk.

Default N/A

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Usage The MBR is the boot sector located at the very beginning of a boot drive. Under advisement from A10 Networks, you can use the command if your compact flash or hard drive cannot boot. If this occurs, boot from the other drive, then use this command.

bootimage

Description Specify the boot image location from which to load the system image the next time the ACOS device is rebooted.

Syntax

```
bootimage {cf pri | hd {pri | sec}}
```

Parameter	Description
cf | **hd**	Boot medium. The ACOS device always tries to boot using the hard disk (**hd**) first. The compact flash (**cf**) is used only if the hard disk is unavailable.
pri | **sec**	Boot image location, primary or secondary.

Default The default location is **primary**, for both the hard disk and the compact flash.

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command configures the ACOS device to boot from the secondary image area on the hard disk the next time the device is rebooted:

```
ACOS(config)# bootimage hd sec
Secondary image will be used if system is booted from hard
disk
ACOS(config)#
```

bpdu-fwd-group

Description Configures a group of tagged Ethernet interfaces for forwarding Bridge Protocol Data Units (BPDUs). BPDU forwarding groups enable you to use the ACOS device in a network that runs Spanning Tree Protocol (STP).

A BPDU forwarding group is a set of tagged Ethernet interfaces that will accept and broadcast STP BPDUs among themselves. When an interface in a BPDU forwarding group receives an STP BPDU (a packet addressed to MAC address 01-80-C2-00-00-00), the interface broadcasts the BPDU to all the other interfaces in the group.

Syntax

```
[no] bpdu-fwd-group group-num
```

Replace group-num with the BPDU forwarding group number (1-8).

If the ACOS device is a member of an aVCS virtual chassis, specify the group number as follows: *DeviceID*/*group-num*

This command changes the CLI to the configuration level for the BPDU forwarding group, where the following command is available.

```
[no] ethernet portnum [to portnum] [ethernet portnum]
```

This command enables you to specify the ethernet interfaces you want to add to the BPDU forwarding group.

Default None

Mode Configuration mode

Usage This command is specifically for configuring VLAN-tagged interfaces to accept and forward BPDUs.

Rules for trunk interfaces:

- BPDUs are broadcast only to the lead interface in the trunk.
- If a BPDU is received on an Ethernet interface that belongs to a trunk, the BPDU is not broadcast to any other members of the same trunk.

Example The following commands create BPDU forwarding group 1 containing Ethernet ports 1-3, and verify the configuration:

```
ACOS(config)# bpdu-fwd-group 1
ACOS(config-bpdu-fwd-group:1)# ethernet 1 to 3
ACOS(config-bpdu-fwd-group:1)# show bpdu-fwd-group
BPDU forward Group 1 members: ethernet 1 to 3
```

bridge-vlan-group

Description Configures a bridge VLAN group for VLAN-to-VLAN bridging.

Syntax

```
[no] bridge-vlan-group group-num
```

Replace *group-num* with the bridge VLAN group number.

If the ACOS device is a member of an aVCS virtual chassis, specify the group number as follows: *DeviceID/group-num*

This command changes the CLI to the configuration level for the specified bridge VLAN group, where the following configuration commands are available:

Command	Description
forward-all-traffic	Configures the bridge VLAN group to be able to forward all kinds of traffic.
forward-ip-traffic	Configures the bridge VLAN group to be able to typical traffic between hosts, such as ARP requests and responses. This is the default setting.
[**no**] **name** *string*	Specifies a name for the group. The string can be 1-63 characters long. If the string contains blank spaces, use double quotation marks around the entire string. There is no default name set.
[**no**] **router-interface ve** *num*	Adds a Virtual Ethernet (VE) interface to the group. This command is applicable only on ACOS devices deployed in routed (gateway) mode. The VE number must be the same as the lowest numbered VLAN in the group. By default this is not set.
[**no**] **vlan vlan-id** [**vlan** *vlan-id* ... | **to vlan** *vlan-id*]	Adds VLANs to the group. By default this is not set.

Default By default, the configuration does not contain any bridge VLAN groups. When you create a bridge VLAN group, it has the default settings described above.

Mode Configuration mode

Usage VLAN-to-VLAN bridging is useful in cases where reconfiguring the hosts on the network either into the same VLAN, or into different IP subnets, is not desired or is impractical.

In bridge VLAN group configurations, the VE number must be the same as the lowest numbered VLAN in the group.

For more information, see"VLAN-to-VLAN Bridging" chapter in the *Network Configuration Guide*.

chassis-application-type

Description The command is used to set the application type on a dual Multi-PU platform box. The command is applicable only to FTA-devices

Syntax `chassis-application-type [adc | cgn]`

Default `cgn`

Mode All

Usage It is mandatory to configure the `chassis-application-type` as `adc` or `cgn` before configuring any other command. The box should be rebooted to switch between the modes.
While switching the box from CGN to ADC, ADC related configuration should not exist on the box on any of the partitions (shared/L3v/service). Execute the `chassis-application-type` command as `adc` and save the configuration.
Similarly, to configure the box for CGN, run the `chassis-application-type` command as `cgn` and save the configuration. CGN related configuration should not exist on the box on any of the partitions (shared/L3v/service).

NOTE: To save the `chassis-application-type` in the startup config, execute `write memory` command.

Example

```
ACOS(config)#chassis-application-type adc
```

class-list

Description Configure a classification list.

Syntax

```
[no] class-list name [ ac | dns | ipv4 | ipv6 | string |
string-case-insensitive ] [ file ]
```

Parameter	Description
name	Specify the name of the class-list.
ac	Create an Aho-Corasick class-list. For more information, see class-list (for Aho-Corasick).
dns	Create a DNS class-list. For more information, see class-list (for VIP-based DNS caching) .
ipv4	Create an IPv4/IPv6 class list. For more information, see class-list (for many pools, non-LSN)
ipv6	
string	Create a string class-list. For more information, see class-list (string).
string-case-insens-itive	Create a cast-insensitive string class-list. For more information, see class-list (string-case-insensitive).
file	Create the class-list as a standalone file on the ACOS device. This option must be configured if the class list needs to be exported.

Mode Global configuration

Usage If you delete a file-based class list (**no class-list** *name*), save the configuration (write memory) to complete the deletion.

NOTE: While creating a class-list as a file, you must configure at least one entry. Else, after reloading or rebooting, a parse error will occur, and the empty class-list file configuration will disappear.

class-list (for Aho-Corasick)

Description Configure an Aho-Corasick class list. This type of class list can be used to match on Server Name Indication (SNI) values.

Syntax

```
[no] class-list list-name ac [file]
```

Parameter	Description
list-name	Adds the list to the running-config.
ac	Identifies this as an Aho-Corasick class list.
file	Saves the list to a standalone file on the ACOS device. This option must be used in order for a class list to be exported.

This command changes the CLI to the configuration level for the specified class list, where the following commands are available:

Command	Description
[no] contains *sni-string*	Matches if the specified string appears anywhere within the SNI value.
[no] ends-with *sni-string*	Matches only if the SNI value ends with the specified string.
[no] equals *sni-string*	Matches only if the SNI value completely matches the specified string.
[no] starts-with *sni-string*	Matches only if the SNI value starts with the specified string.

(The other commands are common to all CLI configuration levels.)

Default None

Mode Configuration mode

Usage The match options are always applied in the following order, regardless of the order in which the rules appear in the configuration.

- Equals
- Starts-with
- Contains
- Ends-with

If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and an SNI value matches on more than one of them, the most-specific match is always used.

If you delete a file-based class list, save the configuration (write memory) to complete the deletion.

class-list (for IP limiting)

Description Configure an IP class list for use with the IP limiting feature.

Syntax

```
[no] class-list list-name [file]
```

Parameter	Description
list-name	Adds the list to the running-config.
file	Saves the list to a standalone file on the ACOS device. This option must be used in order for a class list to be exported.

NOTE: A class list can be exported only if you use the `file` option.

This command changes the CLI to the configuration level for the specified class list, where the following commands are available: .

Parameter	Description
ipv4addr [*/mask-length*] [*ip-limiting-*	Specifies the IPv4 host or subnet address of the client in standard CIDR notation. To configure a wildcard IP address, specify

Parameter	Description
rule]	`0.0.0.0 /0`. The wildcard address matches on all addresses that do not match any entry in the class list. The following *ip-limiting-rule* options are available: • `glid` *num* - Use the specified GLID as the IP limiting rule. • `lid` *num* - Use the specified LID as the IP limiting rule configured at the same level (in the same PBSLB policy template) as the class list. • `lsn-lid` *num* - Use the specified LSN LID as the IP limiting rule. • `lsn-radius-profile` *num* - Use the specified LAN RADIUS profile as the IP limiting rule. To exclude a host or subnet from being limited, do not specify an IP limiting rule.
ipv6addr/*mask-length [ip-limiting-rule]*	Specifies the IPv6 host and subnet address of the client in standard CIDR notation. The available *ip-limiting-rules* are the same as the *ipv4addr* options.

Default None

Mode Configuration mode

Usage Configure the GLIDs or LIDs before configuring the class list entries.

As an alternative to configuring class entries on the ACOS device, you can configure the class list using a text editor on another device, then import the class list onto the ACOS device.

NOTE: If you use a class-list file that is periodically re-imported, the age for class-list entries added to the system from the file does not reset when the class-list file is re-imported. Instead, the entries are allowed to continue aging normally. This is by design.

For more information, see *DDoS Mitigation Guide (for ADC)* for IP limiting.

If you delete a file-based class list (**no class-list** *list-name*), save the configuration (write memory) to complete the deletion.

Request Limiting and Request-Rate Limiting in Class Lists

If a LID or GLID in a class list contains settings for request limiting or request-rate limiting, the settings apply only if the following conditions are true:

1. The LID or GLID is used within a policy template.
2. The policy template is bound to a virtual port.

In this case, the settings apply only to the virtual port. The settings do not apply in any of the following cases:

- The policy template is applied to the virtual server, instead of the virtual port.
- The settings are in a system-wide GLID.
- The settings are in a system-wide policy template.

NOTE: This limitation does not apply to connection limiting or connection-rate limiting. Those settings are valid in all the cases listed above.

Example The following commands configure class list “global”, which matches on all clients, and uses IP limiting rule 1:

```
ACOS(config)# class-list global
ACOS(config-class list)# 0.0.0.0/0 glid 1
```

Related Commands:

- glid
- slb template policy
- import

class-list (for VIP-based DNS caching)

Description Configure an IP class list for use VIP-based DNS caching.

Syntax

```
class-list list-name dns [file]
```

Parameter	Description
list-name	Adds the list to the running-config.
dns	Identifies this list as a DNS class list.
file	Saves the list to a standalone file on the ACOS device. This option must be used in order for a class list to be exported.

This command changes the CLI to the configuration level for the specified class list, where the following command is available:

```
[no] dns match-option domain-string [glid num | lid num]
```

This command specifies the match conditions for domain strings and maps matching strings to LIDs.

Parameter	Description
match-option	Specifies the match criteria for the *domain-string*. The *match-option* can be one of the following: `dns contains` – The entry matches if the DNS request is for a domain name that contains the *domain-string* anywhere within the requested domain name. `dns starts-with` – The entry matches if the DNS request is for a domain name that begins with the *domain-string*. `dns ends-with` – The entry matches if the DNS request is for a domain name that ends with the *domain-string*.

Parameter	Description
domain-string	Specifies all or part of the domain name on which to match. You can use the wildcard character * (asterisk) to match on any single character. For example, "www.example*.com" matches on all the following domain names: www.example1.com, www.example2.com, www.examplea.com, www.examplez.com, and so on. For wildcard matching on more than one character, you can use the `dns contains`, `dns starts-with`, and `dns ends-with` options. For example, "dns ends-with example.com" matches on both abc.example.com and www.example.com.
glid num | *lid num*	Specifies the ID of the IP limiting rule to use for matching clients. You can use a system-wide (global) IP limiting rule or an IP limiting rule configured in a PBSLB policy template. To use an IP limiting rule configured at the Configuration mode level, use the `glid` *num* option. The `lid` *num* option specifies a list ID (LID) in the DNS template. LIDs contain DNS caching policies. The ACOS device applies the DNS caching policy in the specified LID to the *domain-string*. LID and GLID are mutually exclusive, so only configure one or the other.

(The other commands are common to all CLI configuration levels.)

Default None

Mode Configuration mode

Usage Configure the LIDs before configuring the class-list entries. LIDs for DNS caching can be configured in DNS templates. For more information, see "slb template dns" in the *Command Line Interface Reference for ADC*.

As an alternative to configuring class entries on the ACOS device, you can configure the class list using a text editor on another device, then import the class list onto the ACOS device.

If you delete a file-based class list (**no class-list** *list-name*), save the configuration (write memory) to complete the deletion.

For more information, see "DNS Optimization and Security" chapter in the *Application Delivery and Server Load Balancing Guide*.

class-list (for many pools, non-LSN)

Description Configure IP class lists for deployment that use a large number of NAT pools.

Syntax

```
[no] class-list list-name [ipv4 | ipv6] [file]
```

Parameter	Description
list-name	Adds the list to the running-config.
ipv4	Identifies this as an IPv4 class list.
ipv6	Identifies this as an IPv6 class list.
file	Saves the list to a standalone file on the ACOS device. This option must be used in order for a class list to be exported.

This command changes the CLI to the configuration level for the specified class list, where the following commands are available.

```
[no] {ipaddr/network-mask | ipv6-addr/prefix-length}
[ip-limiting-rule]
```

This command adds an entry to the class list.

Parameter	Description
ipaddr **/***network-mask*	Specifies the IPv4 host or subnet address of the client. The *network-mask* specifies the network mask.

Parameter	Description
	To configure a wildcard IP address, specify 0.0.0.0 /0. The wildcard address matches on all addresses that do not match any entry in the class list.
ipv6-addr **/***subnet-length*	Specifies the IPv6 host or network address of the client.
ip-limiting-rule	Specifies the ID of the IP limiting rule to use for matching clients. You can use a system-wide (global) IP limiting rule or an IP limiting rule configured in a PBSLB policy template. • `glid` *num* - Use the specified GLID as the IP limiting rule. • `lid` *num* - Use the specified LID as the IP limiting rule configured at the same level (in the same PBSLB policy template) as the class list. • `lsn-lid` *num* - Use the specified LSN LID as the IP limiting rule. • `lsn-radius-profile` *num* - Use the specified LAN RADIUS profile as the IP limiting rule. To exclude a host or subnet from being limited, do not specify an IP limiting rule.

(The other commands are common to all CLI configuration levels.)

Default None

Mode Configuration mode

Usage First configure the IP pools. Then configure the global LIDs. In each global LID, use the **`use-nat-pool`** *pool-name* command to map clients to the pool. Then configure the class list entries.

As an alternative to configuring class entries on the ACOS device, you can configure the class list using a text editor on another device, then import the class list onto the ACOS device.

If you delete a file-based class list (**no class-list** *list-name*), save the configuration (write memory) to complete the deletion.

For more information, see "Configuring Dynamic IP NAT with Many Pools" section in the *System Configuration and Administration Guide*.

class-list (string)

Description Configure a class list that you can use to modify aFleX scripts, without the need to edit the script files themselves.

Syntax

```
[no] class-list list-name string [file]
```

Parameter	Description
list-name	Adds the list to the running-config.
file	Saves the list to a standalone file on the ACOS device. This option must be used in order for a class list to be exported.
string	Identifies this as a string class list.

Mode Global configuration

Usage If you delete a file-based class list (**no class-list** *list-name*), save the configuration (write memory) to complete the deletion.

For more information, see*aFleX Scripting Language Reference*.

class-list (string-case-insensitive)

Description Configure a cast-insensitive class list that you can use to modify aFleX scripts, without the need to edit the script files themselves.

Syntax

```
[no] class-list list-name string-case-insensitive [file]
```

Parameter	Description
list-name	Adds the list to the running-config.
file	Saves the list to a standalone file on the ACOS device. This option must be used in order for a class list to be exported.
string-case-insensitive	Identifies this as a case-insensitive string class list.

Mode Global configuration

Usage If you delete a file-based class list (**no class-list** *list-name*), save the configuration (write memory) to complete the deletion.

For more information, see *aFleX Scripting Language Reference*.

configure sync

Description Manually synchronize the configurations of all or specific partitions from one ACOS device to other peer-level devices. This command allows configuration synchronization on Shared, L3V, and Service partitions.

Prerequisite

- The destination (peer) device must be reachable and route-able from the current partition.
- While performing synchronization, you must have write privileges on the destination device.
- While using a data port, the enable management service ssh command must be enabled on the data port.

Limitation Following are the limitations while executing this command from L3V and Service partitions:

- Only running and startup configurations are synchronized; while device-specific configurations, such as interface configurations, are not synchronized.
- On Multi-PU platforms, the Configuration Synchronization is not supported.

Syntax

```
[no] configure sync {running | all}
  {{all-partitions | partition name} | {auto-authentication |
private-key name}
dest-ipaddress
```

Parameter	Description
running	Synchronize the local running-config to a peer's running-config.
all	Synchronize the local running-config to a peer's running-config, and the local startup-config to the same peer's startup-config.
all-partitions	Synchronize all partition configurations. **NOTE**: This option is not applicable for configuration synchronization on L3V or Service partitions.
partition *name*	Synchronize the configuration for the specified partition only. **NOTE**: This option is not applicable for configuration synchronization on L3V or Service partitions.
auto-authentication	Authenticate using the local user name and password.
private-key *name*	Authenticate using the specified private key.
dest-ipaddress	IP address of the peer to which you want to synchronize your configurations.

Default N/A

Mode Configuration mode

Usage This command is used to manually synchronize the configurations running-config and startup-config) of all the partitions Shared Partition, L3V Partitions, and Service Partitions from one ACOS device to another ACOS device. Consider a scenario where Thunder devices T1 and T2 are in the VRRP-A environment. Synchronization is possible in the following peer-to-peer scenarios:

- From T1 Shared partition to T2 Shared/L3V/Service partition
- From T1 all partitions including shared to T2 all partitions including shared partitions.
- From T1 L3V partition to and the same T2 L3V partition
- From T1 Service partition to the same T2 Service partition

If synchronization is successful, the following message appears in the log: “Configuration sync to <IP address> succeeded.” If the synchronization fails, the following message appears in the CLI response: “Configuration sync failed.”

Example The following example synchronizes both the local running-config and startup-config for the shared partition only to the peer at IP address 10.10.10.4:

```
ACOS(config)# configure sync all partition shared 10.10.10.4
```

Example The following example of a command synchronizes the running configuration from the p1 partition of the local device to the p1 partition on the peer device with IP address 192.168.105.127:

```
ACOS[p1](config)# configure sync running auto-authentication
192.168.105.127
```

copy

Description Copy a running-config or startup-config.

Syntax

```
copy {running-config | startup-config | from-profile-name}
[use-mgmt-port] {url | to-profile-name}
```

Parameter	Description
running-config	Copies the commands in the running-config to the specified URL or local profile name.
startup-config	Copies the configuration profile that is currently linked to “startup-config” and saves the copy under the specified URL or local profile name.

Parameter	Description
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	Copies the running-config or configuration profile to a remote device. The URL specifies the file transfer protocol, username, and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]`  To enter the entire URL:  • `tftp://host/file` • `ftp://[user@]host[port:]/file` • `scp://[user@]host/file` • `sftp://[user@]host/file`
from-profile-name	Configuration profile you are copying from.
to-profile-name	Configuration profile you are copying to.

NOTE: You cannot use the profile name “default”. This name is reserved and always refers to the configuration profile that is stored in the image area from which the ACOS device most recently rebooted.

Default None

Mode Configuration mode

Usage If you are planning to configure a new ACOS device by loading the configuration from another ACOS device:

1. On the configured ACOS device, use the **copy startup-config** *url* command to save the startup-config to a remote server.
2. On the new ACOS device, use the **copy** *url* **startup-config** command to copy the configured ACOS device’s startup-config from the remote server onto the new ACOS device.
3. Use the **reboot** command (at the Privileged EXEC level) to reboot the new ACOS device.
4. Modify parameters as needed (such as IP addresses).

If you attempt to copy the configuration by copying-and-pasting it from a CLI session on the configured ACOS device, some essential parameters such as interface states will not be copied.

Example The following command copies the configuration profile currently linked to “startup-config” to a profile named “slbconfig3” and stores the profile locally on the ACOS device:

```
ACOS(config)# copy startup-config slbconfig3
```

delete

Description Delete a locally stored file from the ACOS device.

Syntax

```
delete file-type file-name
```

Parameter	Description
file-type	Type of file to be deleted: • **auth-portal** (portal file for HTTP authentication)

Parameter	Description
	• **auth-portal-image** (image file for the default authentication portal) • **auth-saml-idp** (SAML metadata of the identity provider) • **bw-list** (blacklist or whitelist) • **cgnv6 fixed-nat** (fixed-NAT port mapping file) • **cgnv6 lw-4o6-binding-table-validation-log** (lightweight 4over6 binding table validation log) • **debug-monitor** (debug file) • **geo-location** (geo-location file) • **geo-location-class-list** (geo-location class-list file) • **glm-license** (Global Licensing Manager file or temporary license file for a virtual/soft/cloud ACOS device) • **health-external** (external script program) • **health-postfile** (HTTP POST data file) • **local-uri-file** (local URI files for HTTP response) • **ng-waf-custom-page** (custom HTML file for NGWAF) • **partition** (hard delete an L3V partition) • **rpz** (response policy zone file) • **startup-config** (startup configuration profile) • **web-category database** (web-category database) • **threat-intel** (threat-intel files) • **tsig** (Transaction SIGnatures Key file)
file-name	Name of the file you want to delete.

Parameter	Description
	NOTE: • For the **geo-location** option, you can specify **all** instead of a specific *file-name* to delete all files. • There is no file-name option for **web-category database**.

Default N/A

Mode Configuration mode

Usage The **startup-config** file type deletes the specified configuration profile linked to startup-config. The command deletes only the specific profile *file-name* you specify.

If the configuration profile you specify is linked to startup-config, the startup-config is automatically re-linked to the default configuration profile. (The default is the configuration profile stored in the image area from which the ACOS device most recently rebooted.)

Example The following command deletes configuration profile “slbconfig2”:

```
ACOS(config)# delete startup-config slbconfig2
```

disable reset statistics

Description Prevents resetting (clearing) of statistics for the following resources: SLB servers, service groups, virtual servers, and Ethernet interfaces.

Syntax

```
disable reset statistics
```

Default Disabled (clearing of statistics is allowed)

Mode Configuration mode

Usage Admins with the following CLI roles are allowed to disable or re-enable clearing of SLB and Ethernet statistics:

- write
- partition-write

Example The following command disables reset of SLB and Ethernet statistics:

```
ACOS(config)# disable reset statistics
```

disable slb

Description Disable real or virtual servers.

Syntax

```
disable slb server [server-name] [port port-num]

disable slb virtual-server [server-name] [port port-num]
```

Parameter	Description
server-name	Disables the specified real or virtual server.
port *port-num*	Disables only the specified service port. If you omit the *server-name* option, the port is disabled on all real or virtual servers. Otherwise, the port is disabled only on the server you specify.

Default Enabled

Mode Configuration mode

Example The following command disables all virtual servers:

```
ACOS(config)# disable slb virtual-server
```

Example The following command disables port 80 on all real servers:

```
ACOS(config)# disable slb server port 80
```

Example The following command disables port 8080 on real server “rs1”:

```
ACOS(config)# disable slb server rs1 port 8080
```

disable-failsafe

Description Disable fail-safe monitoring for software-related errors.

Syntax

```
[no] disable-failsafe
[all | io-buffer | session-memory | system-memory]
```

Parameter	Description
all	Disables fail-safe monitoring for all the following types of software errors.
io-buffer	Disables fail-safe monitoring for IO-buffer errors.
session-memory	Disables fail-safe monitoring for session-memory errors.
system-memory	Disables fail-safe monitoring for system-memory errors.

Default Fail-safe monitoring and automatic recovery are disabled by default, for both hardware and software errors.

Mode Configuration mode

disable-management

Description Disables management access to the ACOS device.

Syntax `disable-management service {http | https | ntp | ping | snmp | ssh}`

Parameter	Description
http	Disables HTTP access to the management GUI.
https	Disables HTTPS access to the management GUI.
ntp	Disables access to the NTP server on ACOS.
ping	Disables ping replies from ACOS. This option does not affect the ACOS device's ability to ping other devices.
snmp	Disables SNMP access to the ACOS device's SNMP agent.
ssh	Disables SSH access to the CLI.

This command changes the CLI to the configuration level for the type of access you specify. At this level, you can specify the interfaces for which to disable access, using the following options:

- **ethernet** *portnum* [**to** *portnum*]

Disable access for the specified protocol on the specified Ethernet interface. Use the **[to portnum] option to specify a range of Ethernet interfaces.**

- **management**

  Disable access for the specified protocol on the management interface.

- **ve ve-num [to ve-num]**

  Disable access for the specified protocol on the specified virtual Ethernet interface. Use the **[to ve-num] option to specify a range of virtual Ethernet interfaces.**

The CLI lists options only for the interface types for which the access type is enabled by default.

NOTE: Disabling **ping** replies from being sent by the device does not affect the device's ability to ping other devices.

Default Table 11 lists the default settings for each management service.

Table 11 : Default Management Service Settings

Management Service	Ethernet Management Interface	Ethernet and VE Data Interfaces
SSH	Enabled	Disabled
Telnet	Disabled	Disabled
HTTP	Enabled	Disabled
HTTPS	Enabled	Disabled
NTP	Enabled	Enabled
SNMP	Enabled	Disabled
Ping	Enabled	Enabled
Syslog	Disabled	Disabled
SNMP-trap	Disabled	Disabled

Mode Configuration mode

Usage

If you disable the type of access you are using on the interface you are using at the time you enter this command, your management session will end. If you accidentally lock yourself out of the device altogether (for example, if you use the **all** option for all interfaces), you can still access the CLI by connecting a PC to the ACOS device's serial port.

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which to apply this command.

You can enable or disable management access, for individual access types and interfaces. You also can use an Access Control List (ACL) to permit or deny management access through the interface by specific hosts or subnets.

For more information, see "Access Based on Management Interface" in the *Management Access and Security Guide*.

Example

The following command disables HTTP access to the out-of-band management interface:

```
ACOS(config)# disable-management service http management
You may lose connection by disabling the http service.
Continue? [yes/no]: yes
ACOS(config-disable-management http)# management
```

Example

The following command stops ACOS from responding to the incoming NTP client requests on the specified port.

```
ACOS(config)# disable-management service ntp
You may lose connection by disabling the ntp service.
Continue? [yes/no]: yes
ACOS(config-disable-managment ntp)# ethernet 3
```

ACOS stops responding to the incoming NTP client requests on the ethernet 3 port and the status of NTP for ethernet 3 is displayed as "off" in the output of the `show management` command.

Related Commands:

- enable-management

dnssec

dnssec standalone

Description Enable the ACOS device to run DNSSEC without being a member of a GSLB controller group.

Syntax

```
[no] standalone
```

Default Disabled

Mode Configuration mode

Usage GSLB is still required. The ACOS device must be configured to act as a GSLB controller, and as an authoritative DNS server for the GSLB zone.

dnssec template

Description Configure a DNSSEC template.

Syntax

```
[no] dnssec template template-name
```

This command changes the CLI to the configuration level for the specified DNSSEC template, where the following commands are available.

Command	Description
[no] algorithm {RSASHA1 | RSASHA256 | RSASHA512}	Cryptographic algorithm to use for encrypting DNSSEC keys. The default algorithm is RSASHA256.
[no] combinations-limit *num*	Maximum number of combinations per Resource Record Set (RRset), where RRset is defined as all the records of a particular type for a particular domain, such as all the “quad-A” (IPv6) records for www.example.com. You can specify 1-65535. The default number of combinations is 31.

Command	Description
[**no**] **dnskey-ttl** *seconds*	Lifetime for DNSSEC key resource records. The TTL can range from 1-864,000 seconds. The default is 14,400 seconds (4 hours).
[**no**] **enable-nsec3**	Enables NSEC3 support. This is disabled by default.
[**no**] **hsm** *template-name*	Binds a Hardware Security Module (HSM) template to this DNSSEC template.
[**no**] **ksk keysize** *bits*	Key length for KSKs. You can specify 1024-4096 bits. The default is 2048 bits.
[**no**] **ksk lifetime** *seconds* [**rollover-time** *seconds*]	Lifetime for KSKs, 1-2147483647 seconds (about 68 years). The **rollover-time** specifies how long to wait before generating a standby key to replace the current key. The **rollover-time** setting also can be 1-2147483647 seconds. Generally, the **rollover-time** setting should be shorter than the lifetime, to allow the new key to be ready when needed. The default is 31536000 seconds (365 days), with **rollover-time** 30931200 seconds (358 days)
[**no**] **return-nsec-on-failure**	Returns an NSEC or NSEC3 record in response to a client request for an invalid domain. As originally designed, DNSSEC would expose the list of device names within a zone, allowing an attacker to gain a list of network devices that could be used to create a map of the network. This is enabled by default.
[**no**] **signature-validity-period** *days*	Period for which a signature will remain valid. The time can range from 5 to 30 days. The default is 10 days.

Command	Description
[no] **zsk lifetime** *seconds* [**rollover-time** *seconds*]	Lifetime for ZSKs, 1-2147483647 seconds. The **rollover-time** specifies how long to wait before generating a standby key to replace the current key. The **rollover-time** setting also can be 1-2147483647 seconds. Generally, the **rollover-time** setting should be shorter than the lifetime, to allow the new key to be ready when needed. The default is 7776000 seconds (90 days), with **rollover-time** 7171200 seconds (83 days).

Mode Global configuration mode

dnssec dnskey delete

Description Delete DNS Public Key (DNSKEY) resource records.

Syntax **dnssec dnskey delete** [*zone-name*]

Replace *zone-name* with the name of the zone for which to delete DNSKEY resource records. If you do not specify a zone name, the DNSKEY resource records for all child zones are deleted.

Default N/A

Mode Configuration mode

dnssec ds delete

Description Delete Delegation Signer (DS) resource records for child zones.

Syntax **dnssec dnskey delete** [*zone-name*]

Replace *zone-name* with the name of the zone for which to delete DS resource records. If you do not specify a zone name, the DS resource records for all child zones are deleted.

Default N/A

Mode Configuration mode

dnssec key-rollover

Description Perform key change (rollover) for ZSKs or KSKs.

Syntax

```
dnssec key-rollover zone-name
{KSK {ds-ready-in-parent-zone | start} | ZSK start}
```

Parameter	Description
zone-name	Name of the child zone for which to regenerate keys. If you do not specify a zone name, all child zones are re-signed.
KSK {**ds-ready-in-parent-zone** | **start**}	Regenerates key-signing keys (KSKs).: **ds-ready-in-parent-zone** – Indicates that the DS resource record has already been transferred to the parent zone, so it is ok to remove the old active key. **start** – Immediately begins KSK rollover.
ZSK start	Immediately begins ZSK rollover.

Default N/A

Mode Configuration mode

dnssec sign-zone-now

Description Force re-signing of zone-signing keys (ZSKs).

Syntax

```
dnssec sign-zone-now [zone-name]
```

Replace *zone-name* with the name of the child zone for which to re-sign the ZSKs. If you do not specify a zone name, all child zones are re-signed.

Default N/A

Mode Configuration mode

do

Description Run a Privileged EXEC level command from a configuration level prompt, without leaving the configuration level.

Syntax `do command`

Default N/A

Mode Configuration mode

Example The following command runs the **traceroute** command from the Configuration mode level:

```
ACOS(config)# do traceroute 10.10.10.9
```

domain-list

Description Configure the domain classification list.

Syntax `[no] domain-list [domain-list-name]`

This command changes the CLI to the configuration level for the specified domain name list, where the following parameters can be configured:

Parameter	Description
domain-name	Specify a domain name (1-127 characters) to be added to the domain list.
interval *<minutes>*	Specify the query interval (in minutes) for DNS resolution. You can specify a value in the range of 1-1440 minutes. The ACOS device sends DNS queries (A and AAAA type) to the DNS server for resolution. The query interval is the time between DNS queries if the previous query is successful. The default query interval period is 10 minutes.
fail-interval *<seconds>*	Specify the fail-interval (in seconds) for DNS resolution. The DNS fail-interval is the time in seconds that ACOS waits to restart the next DNS query process

Parameter	Description
	for a domain since the last failure. A DNS query process includes a maximum of 5 retry queries sent (for both A and AAAA records) at an interval of 3 seconds if the previous query failed. You can specify the fail-interval in the range of 3-600 seconds. The default fail-interval period is 30 seconds.

Default NA

Mode Global Configuration mode

NOTE: If the query interval and the query fail-interval are not configured explicitly at the domain level, the configuration at the global level (set using the cgnv6 global domain-list command) will take effect.

Example The following command demonstrates command usage. Here, the query interval is set to 4 minutes and the fail-interval is set to 10 seconds.

```
ACOS(config)# domain-list mylist
ACOS(config-domain-list:mylist)# test.a10.com interval 4 fail-interval 10
```

Related Commands:

- cgnv6 global domain-list

enable reset statistics

Description Enable the ability to reset statistics for the following resources: SLB servers, service groups, virtual servers, and Ethernet interfaces.

Syntax

```
enable reset statistics
```

Default Reset statistics is enabled by default.

Mode Configuration mode

Usage Admins with the following CLI roles are allowed to disable or re-enable clearing of SLB and Ethernet statistics:

- write
- partition-write

Example The following command can be used to re-enable the ability to clear SLB and Ethernet statistics, if the disable reset statistics command was used to disable this feature:

```
config)# enable reset statistics
```

enable-core

Description Change the file size of core dumps.

Syntax

```
[no] enable-core {a10 | system}
```

Parameter	Description
a10	Enable A10 core dump files.
system	Enable system core dump files. System core dump files are larger than A10 core dump files.

Default If VRRP-A is configured, system core dump files are enabled by default. If VRRP-A is not configured, A10 core dump files are enabled by default.

Mode Configuration mode

Usage You can save this command to the startup-config on SSD or HD. However, ACOS does not support saving the command to a configuration file stored on Compact Flash (CF). This is because the CF does not have enough storage for large core files.

enable-management

Description Enable management access to the ACOS device.

Syntax

```
[no] enable-management service
{
acl-v4 id |
acl-v6 id |
http |
https |
ntp |
ping |
```

```
snmp |
ssh |
telnet
}
```

Parameter	Description
acl-v4 *id*	Permits or denies management access based on permit or deny rules in the ACL for IPv4 addresses.
acl-v6 *id*	Permits or denies management access based on permit or deny rules in the ACL for IPv6 addresses.
http	Allows HTTP access to the management GUI.
https	Allows HTTPS access to the management GUI.
ntp	Controls access to the NTP server on ACOS.
ping	Allows ping replies from ACOS interfaces. This option does not affect the ACOS device's ability to ping other devices.
snmp	Allows SNMP access to the ACOS device's SNMP agent.
ssh	Allows SSH access to the CLI.
telnet	Allows Telnet access to the CLI.

This command changes the CLI to the configuration level for the type of access you specify. At this level, you can specify the interfaces to enable access and configure additional parameters too. The following options are available:

Parameter	Description
all-data-intf	Enable access to all data interfaces.
ethernet portnum [to portnum]	Enable access to the specified protocol on the specified Ethernet interface. Use the [to portnum] option to specify a range of Ethernet interfaces.
lif lif_name	Enable management access to the specified Logical Interface (LIF). Specify the LIF name (1 to 15 characters).

Parameter	Description
	This option is available for all the services within **enable-management**. Additional Information: • It applies only to incoming management traffic directed to ACOS; outgoing traffic from ACOS remains unchanged and follows existing routing logic. • If **priority** is configured for the service, it is applied only for LIFs that use VLAN tagging (DOT1Q). • A maximum of 16 LIF interfaces can be configured for management access. • A LIF cannot be deleted while a management service is bound to it; it must be unbound first.
management	Enable access to the specified protocol on the management interface.
ve ve-num [to ve-num]	Enable access to the specified protocol on the specified virtual Ethernet interface. Use the [to ve-num] option to specify a range of virtual Ethernet interfaces.
priority	Sets the priority for the management traffic over the data traffic with the access list. This option is disabled by default.

Parameter	Description
	NOTE: The `priority` option is supported only on FTA platforms and applies only to `acl-v4` and `acl-v6` services. If configured, it is applicable to configured VE, Ethernet, DOT1Q LIF, and all data interfaces.

NOTE:

- The management interface supports only a single ACL.
- IPv6 ACLs are supported for management access through Ethernet data interfaces and the management interface.

The CLI lists options only for the interface types for which the access type is disabled by default.

Default The following table lists the default settings for each management service.

Management Service	Management Interface	Data Interfaces
ACL	Enabled	Disabled
HTTP	Enabled	Disabled
HTTPS	Enabled	Disabled
NTP	Enabled	Enabled
Ping	Enabled	Enabled
SNMP	Enabled	Disabled
SSH	Enabled	Disabled
Telnet	Disabled	Disabled

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

For more information, see "Access Based on Management Interface" in the *Management Access and Security Guide*.

Example The following command enables Telnet access to Ethernet data interface 6:

```
ACOS(config)# enable-management service telnet
ACOS(config-enable-management telnet)# ethernet 6
```

Example The following commands configure IPv6 traffic filtering on the management interface and display the resulting configuration:

```
ACOS(config)# ipv6 access-list ipv6-acl1
ACOS(config-access-list:ipv6-acl1)# permit ipv6 any any
ACOS(config-access-list:ipv6-acl1)# exit
ACOS(config)# interface management
ACOS(config-if:management)# ipv6 access-list ipv6-acl1 in
ACOS(config-if:management)# show running-config
ipv6 access-list ipv6-acl1
  permit ipv6 any any
!
interface management
  ip address 192.168.217.28 255.255.255.0
  ipv6 address 2001:192:168:217::28/64
  ipv6 access-list ipv6-acl1 in
```

Example The following commands configure an IPv6 ACL, then apply it to Ethernet data ports 5 and 6 to secure SSH access over IPv6:

```
ACOS(config)# ipv6 access-list ipv6-acl1
ACOS(config-access-list:ipv6-acl1)# permit ipv6 any any
ACOS(config-access-list:ipv6-acl1)# exit
ACOS(config)# enable-management service ssh
ACOS(config-enable-management ssh)# acl-v6 ipv6-acl1
ACOS(config-enable-management ssh-acl-v6)# ethernet 5 to 6
```

Example The following commands configure an ACL for incoming NTP requests on ethernet 1:

```
ACOS(config)# enable-management service ntp
ACOS(config-enable-management ntp)# acl-v4 1
ACOS(config-enable-management ntp-acl-v4)# ethernet 1
```

Example The following commands configure an ACL on all interfaces:

```
ACOS(config)# enable-management service acl-v4 1
ACOS(config-enable-management acl-v4)# ethernet 3
```

An ACL is configured on ethernet 3 and the ACL ID is displayed for all the services of the ethernet 3 in the output of the `show management` command.

Example The following commands configure priority for all the IPv4 management traffic from 10.10.10.10 on the data port 20:

```
ACOS(config)# access-list 100 permit ip 10.10.10.10 /32 any
ACOS(config)# enable-management service acl-v4 100
ACOS(config-enable-management acl-v4)# ethernet 20
ACOS(config-enable-management acl-v4)# priority
```

Example The following commands configure priority for all the IPv6 management traffic on the data port 22:

```
ACOS(config)# ipv6 access-list aclv6-2
ACOS(config-access-list:aclv6-2)# permit ipv6 any any
ACOS(config)# enable-management service acl-v6 aclv6-2
ACOS(config-enable-management acl-v6)# ethernet 22
ACOS(config-enable-management acl-v6)# priority
```

Example The following command binds the HTTPS management service to the specified LIF interface (*lif_test*):

```
ACOS(config)# enable-management service https
ACOS(config-enable-management https)# lif lif_test
```

enable-password

Description Modifies the enable password parameters. Input the password string (1-63) characters after the prompt. Passwords are case sensitive and can contain special characters. (For more information, seeAdding Special Character in Strings.)

If both; password-policy and enable-password follow-password-policy are configured at the system level, the input in this command is checked to ensure that the configured password follows the defined password complexity.

Syntax `enable-password`

Default NA

Mode Configuration mode

Example The following command sets enable password:

```
ACOS(config)# enable-password
Password:
Retype password:
```

NOTE: The password is obfuscated and therefore it is not displayed on the screen.

Related Commands:

- admin
- system password-policy complexity
- system enable-password follow-password-policy

end

Description Return to the Privileged EXEC level of the CLI.

Syntax `end`

Default N/A

Mode Config

Usage The `end` command is valid at all configuration levels of the CLI. From any configuration level, the command returns directly to the Privileged EXEC level.

Example The following command returns from the Configuration mode level to the Privileged EXEC level:

```
ACOS(config)# end
```

```
ACOS#
```

environment temperature threshold

Description Configure the temperature condition under which a log is generated.

Syntax

```
[no] environment temperature threshold low num medium num high num
```

Parameter	Description
low num	Low temperature threshold in Celcius; a log is generated when the temperature drop below this threshold.
medium num	Medium temperature threshold in Celcius.This threshold causes the status in the **show environment** command to change between “low/med” or “med/high”.
high num	High temperature threshold in Celcius; a log is generated when the temperature rises above this threshold.

Default Low is 25, medium is 45, high is 68.

Mode Configuration mode

Example Set the low temperature threshold to 20 degress Celcius, medium to 45 degrees Celcius, and high temperature threshold to 55 degrees Celcius:

```
ACOS(config)# environment temperature threshold low 20 medium 45 high 55
```

The `show environment` command reflects the new temperature thresholds:

```
ACOS(config)# show environment
Updated information every 30 Seconds
Physical System temperature:   38C / 100F : OK-low/med
                Thresholds: Low 20 / Medium 45 / High 55
Physical System temperature2:   34C / 93F : OK-low/med
                Thresholds: Low 20 / Medium 45 / High 55
```

```
HW Fan Setting: Automatic
Fan1A : OK-med/high     Fan1B : OK-med/high
Fan2A : OK-med/high     Fan2B : OK-med/high
Fan3A : OK-med/high     Fan3B : OK-med/high
Fan4A : OK-med/high     Fan4B : OK-med/high
Fan5A : OK-med/high     Fan5B : OK-med/high
Fan6A : OK-med/high     Fan6B : OK-med/high
Fan7A : OK-med/high     Fan7B : OK-med/high
Fan8A : OK-med/high     Fan8B : OK-med/high
System Voltage 12V               : OK
System Voltage 5V                : OK
System Voltage CPU1 VCORE (1V)   : OK
System Voltage CPU0 VCORE (1V)   : OK
System Voltage AUX 5V            : OK
System Voltage VBAT (3.3V)       : OK
Upper Left Power Unit(Rear View) State: On
Upper Right Power Unit(Rear View) State: On
Lower Left Power Unit(Rear View) State: On
Lower Right Power Unit(Rear View) State: Off
```

In addition, both temperature status indicate “low/med” because the temperatures fall in between the low threshold of 20 and medium threshold of 45.

environment update-interval

Description Configure the hardware polling interval for fault detection and log generation.

Syntax

```
[no] environment update-interval num
```

Parameter	Description
num	Polling interval in seconds (1-60). The lower the update interval number, the faster the messages will be seen in the sylog and the status reflected in the **`show environment`** output.

Default 30 seconds

Mode Configuration mode

Example Set the hardware polling interval to 5 seconds:

```
ACOS(config)# environment update-interval 5
```

Use the **show environment** to verify this change, or to view the current hardware polling interval. The first line in the output shows the hardware polling interval:

```
ACOS(config)# show environment
Updated information every 5 Seconds
Physical System temperature:   37C / 98F : OK-med/high
                 Thresholds: Low 10 / Medium 30 / High 45
Physical System temperature2:   32C / 89F : OK-med/high
                 Thresholds: Low 10 / Medium 30 / High 45
HW Fan Setting: Automatic
Fan1A : OK-med/high     Fan1B : OK-med/high
Fan2A : OK-med/high     Fan2B : OK-med/high
Fan3A : OK-med/high     Fan3B : OK-med/high
Fan4A : OK-med/high     Fan4B : OK-med/high
Fan5A : OK-med/high     Fan5B : OK-med/high
Fan6A : OK-med/high     Fan6B : OK-med/high
Fan7A : OK-med/high     Fan7B : OK-med/high
Fan8A : OK-med/high     Fan8B : OK-med/high
System Voltage 12V              : OK
System Voltage 5V               : OK
System Voltage CPU1 VCORE (1V)  : OK
System Voltage CPU0 VCORE (1V)  : OK
System Voltage AUX 5V           : OK
System Voltage VBAT (3.3V)      : OK
Upper Left Power Unit(Rear View) State: On
Upper Right Power Unit(Rear View) State: On
Lower Left Power Unit(Rear View) State: On
Lower Right Power Unit(Rear View) State: Off
```

NOTE: ACOS does not trigger a power-off event until the condition is detected three consecutive times. The event is triggered on the fourth detection, and all values follow this trigger event. FAN reports a status (OK or FAIL) and a speed range (low, med, or high). For example: Fan1A : OK-med/high. Low and high speed ranges follow the trigger event, while OK and FAIL statuses are reported immediately.

erase

Description Erase the startup-config file.

This command returns the device to its factory default configuration after the next reload or reboot.

The following table summarizes that is removed or preserved on the system:

What is Erased	What is Preserved
Saved configuration files	Running configuration
Management IP address	Audit log entries
Admin-configured admins	System files, such as SSL certificates and keys, aFleX policies, black/white lists, and system logs
Enable password	Inactive partitions

To remove imported files or inactive partitions, you must use the **system-reset** command.

Syntax

```
erase [preserve-management] [preserve-accounts] [reload]
```

Parameter	Description
preserve-management	Keeps the configured management IP address and default gateway, instead of erasing them and resetting them to their factory defaults following reload or reboot. The **preserve-management**option only affects the device's network configuration. If it changed the enterprise's organizational structure, there will be a warning advising not to use it.
preserve-accounts	Keeps the configured admin accounts, instead of erasing them. Likewise, this option keeps any modifications to the "admin" account, and does not reset the account to its defaults following reload or reboot.
reload	Reloads ACOS after the configuration erasure is completed. **NOTE:** When performing **erase preserve-management reload**, the management configuration is removed from the current configuration but remains in the system memory, until a reboot is performed.

Default N/A

Mode Configuration mode

Usage The erasure of the startup-config occurs following the next reload or reboot. Until the next reload or reboot, the ACOS device continues to run based on the running-config.

To recover the configuration, you can save the running-config or reload the configuration from another copy of the startup-config file.

Example The following command erases the startup-config file. The change takes place following the next reload or reboot.

```
ACOS(config)# erase
```

Example The following command erases the startup-config file, except for management interface access and admin accounts, and reloads to place the change into effect.

```
ACOS(config)# erase preserve-management preserve-accounts
reload
```

Related Commands:

- system-reset

event

Description Generate an event for the creation or deletion of an L3V partition.

Syntax

```
[no] event partition {part-create | part-del}
```

Parameter	Description
part-create	Generate an event when a partition is created.
part-del	Generate an event when a partition is deleted.

Default N/A

Mode Configuration mode

Related Commands:

- show event-action

exit

Description Return to the Privileged EXEC level of the CLI.

Syntax

```
exit
```

Default N/A

Mode Configuration mode

Usage The **exit** command is valid at all CLI levels. At each level, the command returns to the previous CLI level. For example, from the server port level, the command returns to the server level. From the Configuration

mode level, the command returns to the Privileged EXEC level. From the user EXEC level, the command terminates the CLI session.

From the Configuration mode level, you also can use the **end** command to return to the Privileged EXEC level.

Example The following command returns from the Configuration mode level to the Privileged EXEC level:

```
ACOS(config)# exit
ACOS#
```

fail-safe

Description Configure fail-safe automatic recovery.

Syntax

```
[no] fail-safe
{
dataplane-recovery-timeout seconds
fpga-buff-recovery-threshold 256-buffer-units |
hw-error-monitor-disable
hw-error-monitor-enable |
hw-error-recovery-timeout minutes |
session-memory-recovery-threshold percentage |
sw-error-monitor-enable |
sw-error-recovery-timeout minutes |
total-memory-size-check Gb {kill | log}
}
```

Parameter	Description
dataplane-recovery-*seconds* **timeout**	Number of seconds fail-safe detects the dataplane hung before the ACOS device reboots. You can specify 1-30 seconds.
fpga-buff-recovery-threshold *256-buffer-units*	Minimum required number of free (available) FTA buffers. If the number of free buffers remains below this value until the recovery timeout, fail-safe software recovery is triggered. You can specify 1-10 units. Each unit contains 256 buffers. The default is 2 units (512 buffers).

Parameter	Description
hw-error-monitor-disable	Disables fail-safe monitoring and recovery for hardware errors. This is enabled by default.
hw-error-monitor-enable	Enables fail-safe monitoring and recovery for hardware errors. This is enabled by default.
hw-error-recovery-timeout *minutes*	Number of minutes fail-safe waits after a hardware error occurs to reboot the ACOS device. You can specify 1-1440 minutes. The default is 0 (not set).
session-memory-recovery-threshold *percentage*	Minimum required percentage of system memory that must be free. If the amount of free memory remains below this value long enough for the recovery timeout to occur, fail-safe software recovery is triggered. You can specify 1-100 percent. The default is 30 percent. **NOTE:** **fail-safe sw-error-monitor-enable** must be configured to trigger the session memory recovery threshold.
sw-error-monitor-enable	Enables fail-safe monitoring and recovery for software errors. This is disabled by default.
sw-error-recovery-timeout *minutes*	Number of minutes (1-1440) the software error condition must remain in effect before fail-safe occurs: • If the system resource that is low becomes free again within the recovery timeout period, fail-safe allows the ACOS device to continue normal

Parameter	Description
	operation. Fail-safe recovery is not triggered. • If the system resource does not become free, then fail-safe recovery is triggered. The default timeout is 3 minutes.
total-memory-size-check *Gb* {**kill** | **log**}	Amount of memory the device must have after booting. • *Gb* - Minimum amount of memory required. • **kill** – Stops data traffic and generates a message. However, the management port remains accessible. • **log** – Generates a log message but does not stop data traffic.

Default By default, fail-safe automatic recovery is enabled for hardware errors and disabled for software errors. You can enable the feature for hardware errors, software errors, or both. When you enable the feature, the other options have the default values described in the table above.

Mode Configuration mode

Usage Fail-safe hardware recovery also can be triggered by a “PCI not ready” condition. This fail-safe recovery option is enabled by default and can not be disabled.

fan-speed

Description Configure the fan speed settings (only in A10 Thunder FTA hardware devices).

NOTE: This command is provided as a debug feature for A10 devices placed in lab environments that are in close proximity to the users. A10 does not recommend the default setting (**auto**) be ever changed in a production environment where the A10 product is correctly racked in a Datacenter.

The A10 hardware devices that support this command as listed below:

- Thunder 14045
- Thunder 7650/7655
- Thunder 3350
- Thunder 5840/5845
- Thunder 7440/7445

Syntax

```
fan-speed [ auto | 50 | 75 | 100 ]
```

Parameter	Description
`auto`	Sets the fan speed automatically based on the system temperature. This is the default and recommended setting.
`50`	Sets the fan speed to 50% of the maximum speed.
`75`	Sets the fan speed to 75% of the maximum speed.
`100`	Sets the fan speed to 100% capacity i.e., full hardware speed. **NOTE:** This setting will reduce the operation lifespan of the fan.

Mode Configuration

Default `auto`

Usage Use this command to adjust the fan speed only in situations where the A10 device is not installed correctly in the Datacenter rack.

Example The following command sets the fan speed to 75% of the maximum capacity:

```
ACOS(config)# fan-speed 75
```

file-system

Description Manage the log files present in the specified system directory.

Syntax

```
file-system [ a10log | syslog | varlog ] rm file_name
```

Parameter	Description
a10log	Manage the logs present in the **a10log** directory. This directory contains showtech and support files.
syslog	Manage the logs present in the **syslog** directory. This directory contains Linux system logs.
varlog	Manage the logs present in the **varlog** directory. This directory contains ACOS system logs.
rm *file_name*	Delete the specified file (1-128 characters). **NOTE:** Directories cannot be deleted using this command.

Mode All

Usage Use the **show file-system** command to view the log file information for any of the system directories (**a10log/syslog/varlog**) and then use the **file-system rm** command to delete a particular log (present in the system directory).

NOTE: This command is not supported on the Thunder Container platform.

Example The following command deletes *clear.log* present in **syslog** directory:

```
ACOS(config)# file-system syslog rm clear.log
```

glid

Description Configure a global set of IP limiting rules for system-wide IP limiting.

This command configures a limit ID (LID) for use with the IP limiting feature. For more information, see *IPv4-to-IPv6 Transition Solutions Guide* to configure a LID for use with Large-Scale NAT (LSN) instead.

Syntax

```
[no] glid num
```

Replace num with the limit ID (1-1023).

The command changes the CLI to the configuration level for the specified global LID, where these commands are available. (The other commands are common to all CLI configuration levels.)

Command	Description
[**no**] **conn-limit** *num*	Specifies the maximum number of concurrent connections allowed for a client. You can specify 0-1048575. Connection limit 0 immediately locks down matching clients. There is no default value set for this parameter.
[**no**] **conn-rate-limit** *num* **per** *num-of-100ms*	Specifies the maximum number of new connections allowed for a client within the specified limit period. You can specify 1-4294967295 connections. The limit period can be 100-6553500 milliseconds (ms), specified in increments of 100 ms. There is no default value set for this parameter.
[**no**] **dns** *options*	Configure settings for IPv4 DNS features. the following options are available: • **cache-disable** – Disables DNS cache. • **cache-enable** – Enables DNS cache. • **ttl** – Specifies the period for which an entry remains in the cache before it is removed. A value can be set from 1 to 65535. • **weight** – Sets DNS cache entry weight. Value can be assigned from 1 to 7. The default weight is 1. The specified weight deletes the entries as mentioned below: ◦ If the cache is more than 60% full, entries with weight 1 are eligible to be deleted. ◦ If the cache is more than 70% full, entries with weight 1 or 2 are eligible to be deleted. ◦ If the cache is more than 80% full, entries with

Command	Description
	weights 1-4 are eligible to be deleted. ◦ If the cache is more than 90% full, entries with weights 1-6 are eligible to be deleted.
[**no**] **dns64** *options*	Configure settings for IPv6 DNS features. The following options are available: • **disable** • **exclusive-answer** • **IPv6 prefix** For details, see glid (for NAT64 override).
[**no**] **over-limit-action** [**forward** | **reset**] [**lockout** *minutes*] [**log** *minutes*]	Specifies the action to take when a client exceeds one or more of the limits. The command also configures lockout and enables logging. Action can include: • **drop** – The ACOS device drops that traffic. If logging is enabled, the ACOS device also generates a log message. (There is no **drop** keyword; this is default action.) • **dns-cache-disable** – Disables dns cache when the client exceeds the specified limit. You can specify the lockout period for this option and also enable logging. • **dns-cache-enable** – Enables dns cache when the client exceeds the specified limit. You can specify the lockout period for this option and also enable logging. • **forward** – The ACOS device forwards the traffic. If logging is enabled, the ACOS device also generates a log message. • **lockout** – Specifies the number of minutes during

Command	Description
	which to apply the over-limit action after the client exceeds a limit. The lockout period is activated when a client exceeds any limit. The lockout period can be 1-1023 minutes. There is no default lockout period. • **log** – Generates log messages when clients exceed a limit. When you enable logging, a separate message is generated for each over-limit occurrence, by default. You can specify a logging period, in which case the ACOS device holds onto the repeated messages for the specified period, then sends one message at the end of the period for all instances that occurred within the period. The logging period can be 0-255 minutes. The default is 0 (no wait period). • **reset** – For TCP, the ACOS device sends a TCP RST to the client. If logging is enabled, the ACOS device also generates a log message.
[**no**] **request-limit** *num*	Specifies the maximum number of concurrent Layer 7 requests allowed for a client. You can specify 1-1048575.
[**no**] **request-rate-limit** *num* **per** *num-of-100ms*	Specifies the maximum number of Layer 7 requests allowed for the client in the specified limit period. You can specify 1-4294967295 connections. The limit period can be 100-6553500 milliseconds (ms), specified in 100 ms increments.
[**no**] **use-nat-pool** *pool-name*	Binds a NAT pool to the GLID. The pool is used to provide reverse NAT for class-list members that are mapped to this GLID. (The use-nat-pool option, available in GLIDs, is applicable only to transparent traffic, not to SLB traffic.)

Mode Configuration mode

Usage This command uses a single class list for IP limiting. To use multiple class lists for system-wide IP limiting, use a policy template instead.

Differences Between GLIDs and LIDs

A Global Limit ID (GLID) is an ID that identifies a set of limiting rules configured globally. This ID is included in a class-list, as shown in the following example:

```
glid 10
  request-limit 100
class-list HTTP-RL
  10.100.0.0/16 lid 1
  10.2.0.0/16 lid 2
  0.0.0.0/0 glid 10
```

The limiting rules within a GLID can be reused in different class-list objects, unlike a Local Limit ID (LID).

A LID is an ID that identifies a set of limiting rules configured inside an SLB template of a certain type, such as an SLB policy template or an SLB DNS template, that support a class-list. For example:

```
slb template policy Policy-HTTP-RL
  class-list HTTP-RL
    lid 1
      request-limit 1000
    lid 2
      request-limit 10
```

A local limit ID can be used if the same class-list is used for several different VIPs, and if each VIP has different limiting rules; using the LID eliminates the need to create many class-lists.

Note that GLIDs and LIDs are optional configurations within a class-list, and they are not required if the class-list is used as a black-list or a white-list.

Additional Usage Information about GLIDs and LIDs

A policy template is also required if you plan to apply IP limiting rules to individual virtual servers or virtual ports.

The **request-limit** and **request-rate-limit** options apply only to HTTP, fast-HTTP, and HTTPS virtual ports. For more information, see Request Limiting and Request-Rate Limiting in Class Lists.

The `over-limit-action log` option, when used with the **`request-limit`** or **`request-rate-limit`** option, always lists Ethernet port 1 as the interface.

The **`use-nat-pool`** option is applicable only to transparent traffic, not to SLB traffic.

Example The following commands configure a global IP limiting rule to be applied to all IP clients (the clients that match class list "global"):

```
ACOS(config)# glid 1
ACOS(config-glid:1)# conn-rate-limit 10000 per 1
ACOS(config-glid:1)# conn-limit 2000000
ACOS(config-glid:1)# over-limit forward logging
ACOS(config-glid:1)# exit
ACOS(config)# system glid 1
ACOS(config)# class-list global
ACOS(config-class list)# 0.0.0.0/0 glid 1
```

Related Commands:

- slb template policy

glm

Description Manually enable a connection to the Global License Manager.

Syntax

```
[no] glm enable-requests
```

Default Disabled

Mode Configuration mode

For a complete list of glm commands, refer to the *Capacity FlexPool License and Enterprise License Management User Guide.*

hd-monitor enable

Description Enables hard disk monitoring on your ACOS device.

Syntax

```
[no] hd-monitor enable
```

Default Hard disk monitoring is disabled by default.

Mode Configuration mode

Example The example below shows how to enable hard disk monitoring.

```
ACOS(config)# hd-monitor enable
Harddisk monitoring turned on.
Please write mem and reload to take effect.
ACOS(config)#
```

NOTE: When the `hd-monitor` command is enabled, a process starts in the background and writes 4KB of random data to the root file system. If the written data and the backup data are the same, no error displays. Else, the console log "HDMonitor: Unable to write to the hard drive" is created, which will be followed by a reboot.

health global

Description Globally change health monitor parameters.

Syntax

```
health global
```

This command changes the CLI to the configuration level for global health monitoring parameters, where the following commands are available.

Command	Description
[no] check-rate *threshold*	Change the health-check rate limiting threshold. Replace *threshold* with the maximum number of health-check packets the ACOS device will send in a given 500-millisecond (ms) period. When auto-adjust mode is enabled, you cannot manually change the threshold. To change the threshold, you first must disable auto-adjust mode.
[no] disable-auto-adjust	Disable the auto-adjust mode of health-check rate limiting. When necessary, the auto-adjust mode dynamically increases the default interval and timeout for health checks. By increasing these timers, health-check rate limiting provides more time for health-check

Command	Description
	processing. Auto-adjust mode is enabled by default.
[**no**] **external-rate** *scripts* **per** *100-ms-units*	Specify the maximum number of external health-checks scripts the ACOS device is allowed to perform during a given interval. • *scripts* – Maximum number of scripts. • *100-ms-units* – Interval to which *scripts* option applies.
interval *i-sec* **[timeout** *t-sec***]**	A health check attempt consists of the ACOS device sending a packet to the server. The packet type and payload depend on the health monitor type. For example, an HTTP health monitor might send an HTTP GET request packet. • *i-sec* – period between health check attempts (seconds). • *t-sec* – period ACOS waits for a reply to a health check (seconds). This value must be less than or equal to *i-sec*. **NOTE:** The **timeout** parameter is not applicable to external health monitors.
multi-process *num*	Enable multiple CPUs for health monitoring processes. The default setting is 1 CPU. Replace *num* to assign multiple CPUs to the health monitoring processes. This number cannot exceed the number of configured control CPU's. **NOTE:** It is recommended to set the value to the same number of control CPU's.
retry *number*	Maximum number of times ACOS will send the same health check to an unresponsive server before

Command	Description
	determining that the server is down.
up-retry *number*	Number of consecutive times the device must pass the same periodic health check, in order to be marked Up.

Mode Configuration mode

Usage Globally changing a health monitor parameter changes the default for that parameter. For example, if you globally change the interval from 5 seconds to 10 seconds, the default interval becomes 10 seconds.

To restore the global parameter to its default, use the "no" form of the command. For example, **no up-retry 10**.

If a parameter is explicitly set on a health monitor, globally changing the parameter does not affect the health monitor. For example, if the interval on health monitor hm1 is explicitly set to 20 seconds, the interval remains 20 seconds on hm1 regardless of the global setting.

NOTE: Modifying the global health monitor parameter automatically applies to all the newly configured health monitor as well. To apply a global health monitor parameter change to health monitors that were configured before the change, you must reboot the ACOS device.

Example The following command globally changes the default number of retries to 5:

```
ACOS(config)# health global
ACOS(config-health:global)# retry 5
```

Example This command globally changes the interval and timeout to 10 seconds.

```
ACOS(config-health:global)# interval 10 timeout 10
```

health monitor

Description Configure a health monitor.

Syntax

```
[no] health monitor monitor-name
```

This command changes the CLI to the configuration level for the health monitor. See *Related Commands* below.

Mode Global configuration

Related Commands:

- default-state-up
- disable-after-down
- dsr-l2-strict
- header-insert
- interval
- method
- override-ipv4
- override-ipv6
- override-port
- passive
- proxy-header
- retry
- server-ssl
- ssl-ciphers
- ssl-ticket
- ssl-version
- strictly-retry-on-server-error-response
- up-retry

health source-nat

Description Configure source NAT for health check traffic from specified NAT pool.

Syntax

```
[no] health source-nat
```

This command activates the health source NAT configuration mode where the following commands are available.

Parameter	Description
source-nat-pool *<pool-name>*	Specifies the name of the source NAT pool for IPv4 traffic.
source-nat-pool-v6 *<pool-name-v6>*	Specifies the name of the source NAT pool for IPv6 traffic.
smart-nat-precedence [vrid*<vrid-value>***]**	Configures ACOS using smart NAT for the source NAT address. If smart-nat-precedence is configured, Smart NAT is prioritized over source NAT pools for health check traffic. If VRRP ID not configured, default VRRP ID is used for smart NAT precedence option.
enable-vrrp-a-mode interface *<ethernet|ve|trunk><intf-num>*	Specifies the interface that connects to peer ACOS device in VRRP. This ensures that the ACOS device forwards the health check packets to real servers only in the VRRP active state.

Mode Global Cconfiguration mode

Usage This command configures source NAT for health check traffic that passes through the ACOS device. ACOS enables the active device use a single source IP address for health check traffic, leveraging NAT pools or smart NAT instead of the interface IPs of individual devices.

Example The following command configures source NAT pools, enables smart NAT precedence, and ensures health checks are forwarded by the active ACOS device in a VRRP setup.

```
ACOS(config)#health source-nat
ACOS(config-health:source-nat)#source-nat-pool sn
ACOS(config-health:source-nat)#source-nat-pool-v6 sn6
ACOS(config-health:source-nat)#smart-nat-precedence
```

```
ACOS(config-health:source-nat)#enable-vrrp-a-mode interface
ethernet 3
!
```

health-test

Description Test the status of a device at a specified IP address using a defined health monitor.

To configure a health monitor, use the health monitor command.

Syntax

```
health-test ipaddr [count num] [monitorname name] [port
portnum]
```

Parameter	Description
ipaddr	IPv4 or IPv6 address of the device you want to test.
count *num*	Wait for count tests (1-65535). The default count is 1.
monitorname *name*	Specify the pre-configured health monitor to use for the test.
port *portnum*	Specify the port to test.

Mode Configuration mode

hostname

Description Set the ACOS device's hostname.

Syntax

```
[no] hostname string
```

Replace string with the desired hostname (1-31 characters). The name can contain any alpha-numeric character (a-z, A-Z, 0-9), hypen (-), period (.), or left or right parentheses characters.

Default The default hostname is the name of the device; for example, an AX Series 5630 device will have "AX5630" as the default hostname.

Mode Configuration mode

Usage The CLI command prompt also is changed to show the new hostname.

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in chassis to which this command must apply.

Example The following example sets the hostname to “SLBswitch2”:

```
ACOS(config)# hostname SLBswitch2
SLBswitch2(config)#
```

hsm template

Description Configure a template for DNSSEC or SSL Hardware Security Module (HSM) support.

Syntax

```
[no] hsm template template-name {softHSM | thalesHSM}
```

Replace *template-name* with the name of the template (1-63 characters).

This command changes the CLI to the configuration level for the specified template, where the following command is available for both template types:

password *hsm-passphrase*

This command configures the HSM passphrase.

hsm template *template-name* softHSM

Description Configure a template for DNSSEC Hardware Security Module (HSM) support.

Syntax

```
[no] hsm template template-name softHSM
```

Replace *template-name* with the name of the template (1-63 characters).

The other commands at this level are common to all CLI configuration levels. See Global.

Default Not set

Mode softHSM template mode

hsm template *template-name* thalesHSM

Description Configure a template for Thales SSL Hardware Security Module (HSM) device support.

Syntax

```
[no] hsm template template-name thalesHSM
```

This command changes the CLI to the configuration level for thalesHSM, where the following Thales-specific commands are available:

Command	Description
[no] hsm-ip [port | priority]	Specify the IPv4 address of the Thales hardware device. • port: The port for communicating with the device <1-65535>. • priority: In the case of configuring multiple devices, specify the priority of each device <1-100>.
[no] rfs-ip [port]	Specify the IPv4 address of the Thales remote file system where the encryption keys are stored. • port: The port for communicating with the device <1-65535>.
[no] protection	Specify the authentication protection method between the ACOS device and the Thales HSM device: • module • ocs • softcard Currently only the Thales HSM setting of Operator Card Set (ocs) is supported.
[no] worker	Specify the number of workers for each data CPU. You can select 1-31 for the poll thread number of each data CPU. For higher end models, you can specify the higher numbers in the available range. The higher the number, the more threads and queues dedicated to pull from Thales HSM.

Command	Description
[**no**] health-check-interval	Specify the health check interval for verifying if the HSM device is live. You can select 3-60 seconds (default 10).
[**no**] sec-world	Specify the Thales security world name if you're using a non-default sec-world name in your Thales architecture (1-128 characters).

Default Not set

Mode thalesHSM template mode

Usage This command configures a global Thales HSM template for use with binding to the `slb template client-ssl` command.

Example The following example creates a Thales HSM template called "example_name" then assigns it IP addresses and protection that match the Thales HSM settings.

```
ACOS(config)# hsm template example_name thalesHSM
ACOS(config-template:example_name)# hsm-ip 192.168.213.130
ACOS(config-template:example_name)# rfs-ip 192.168.213.78
ACOS(config-template:example_name)# protection ocs
```

icmp-rate-limit

Description Configure ICMP rate limiting, to protect against denial-of-service (DoS) attacks.

Syntax `[no] icmp-rate-limit normal-rate lockup max-rate lockup-time`

Parameter	Description
normal-rate	Maximum number of ICMP packets allowed per second. If the ACOS device receives more than the normal rate of ICMP packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.

Parameter	Description
lockup *max-rate*	Maximum number of ICMP packets allowed per second before the ACOS device locks up ICMP traffic. When ICMP traffic is locked up, all ICMP packets are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the ACOS device drops all ICMP traffic, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

Default None

Mode Configuration mode

Usage This command configures ICMP rate limiting globally for all traffic to or through the ACOS device. The icmp-rate-limit command is used to configure ICMP rate limiting on individual Ethernet interfaces. The slb template virtual-server command is used to configure ICMP rate limiting in a virtual server template. If you configure ICMP rate limiting filters at more than one of these levels, all filters are applicable.

Specifying a maximum rate (lockup rate) and lockup time is optional. If you do not specify them, lockup does not occur.

Log messages are generated only if the lockup option is used and lockup occurs. Otherwise, the ICMP rate-limiting counters are still incremented but log messages are not generated.

Example The following command globally configures ICMP rate limiting to allow up to 2048 ICMP packets per second, and to lock up all ICMP traffic for 10 seconds if the rate exceeds 3000 ICMP packets per second:

```
ACOS(config)# icmp-rate-limit 2048 lockup 3000 10
```

icmpv6-rate-limit

Description Configure ICMPv6 rate limiting for IPv6 to protect against denial-of-service (DoS) attacks.

Syntax

```
[no] icmpv6-rate-limit normal-rate lockup max-rate lockup-time
```

Parameter	Description
normal-rate	Maximum number of ICMPv6 packets allowed per second. If the ACOS device receives more than the normal rate of ICMPv6 packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.
lockup *max-rate*	Maximum number of ICMPv6 packets allowed per second before the ACOS device locks up ICMPv6 traffic. When ICMPv6 traffic is locked up, all ICMPv6 packets are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the ACOS device drops all ICMPv6 traffic, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

Default None

Mode Configuration mode

Usage This command configures ICMPv6 rate limiting globally for all traffic to or through the ACOS device. The icmpv6-rate-limit command is used to configure ICMPv6 rate limiting on individual Ethernet interfaces. The slb template virtual-server command is used to configure it in a virtual server template. If you configure ICMPv6 rate limiting filters at more than one of these levels, all filters are applicable.

Specifying a maximum rate (lockup rate) and lockup time is optional. If you do not specify them, lockup does not occur.

Log messages are generated only if the lockup option is used and lockup occurs. Otherwise, the ICMPv6 rate-limiting counters are still incremented but log messages are not generated.

import

Description Get a file from a remote site.

Syntax

```
import file-type options
```

Parameter	Description
aflex *file_options1*	Import an aFleX file. **Syntax:** **aflex** *filename* {[**user-tag** *user-tag-name*] [**proxy** *host:port*] [**overwrite**] [**use-mgmt-port**] {*url* | *import-store-name* | **terminal**} **Parameters:** • *filename* - local file name (1-63 characters) • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the aFleX file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. • **overwrite** - Enables the overwriting of existing files of the same local name. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
auth-jwks *file_options1*	Import a JSON web key file for Application Access Management (AAM).

Parameter	Description
	For the *file_options1* syntax, see **aflex** *file_options1*.
auth-portal *file_options1*	Import an authentication portal file for Application Access Management (AAM). For the *file_options1* syntax, see **aflex** *file_options1*.
auth-portal-image *file_options1*	Import an image file for the default authentication portal. For the *file_options1* syntax, see **aflex** *file_options1*.
auth-saml-idp *file_options2*	Import the SAML metadata of the identity provider. **Syntax:** **auth-saml-idp** *metadata-name* [**verify-xml-signature**] [**proxy** *host:port*] [**overwrite**] [**use-mgmt-port**] *url* **Parameters:** • *metadata-name* - Local SAML metadata name (1-63 alphanumeric characters) • **verify-xml-signature** - Verify metadata's XML signature • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the SAML metadata file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, [a:b::1]:8080

Parameter	Description
	◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - Enables the overwriting of existing metadata of the same local name • **use-mgmt-port** - See use-mgmt-port below. • *url* - See *url* below.
bw-list *file_options1*	Import a black/white list. For the *file_options1* syntax, see **aflex** *file_options1*.
ca-cert *file_options3*	Imports a CA certificate without a key. ACOS distinguishes between a *CA cert* and an *SSL cert* which is imported using the syntax **cert** *file_options3*. CA certs are not used for handshaking with SSL clients. **Syntax:** **ca-cert {bulk |** *filename*} [**certificate-type** {**pem** | **der** | **pfx** | **p7b**}] [pfx-password *pswd*] **[overwrite] [user-tag** *user-tag-name*] **[use-mgmt-port]** {*url* | *import-store-name* | **terminal}** **Parameters:** • Use the **bulk** option to import multiple files simultaneously as a .tgz archive. ◦ *filename* - local file name (1-255 alphanumeric characters) • Use **certificate-type** {**pem** | **der** | pfx | **p7b**} to specify a certificate type. • Use pfx-password *pswd* to specify the PFX certificated password if and only if you have specified the **pfx** certificate type.

Parameter	Description
	• **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. The **overwrite** option enables the overwriting of an existing bulk file or an existing file of the same local name. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See url below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
cert *file_options3*	Imports an SSL certificate file. ACOS distinguishes between a *CA cert* and an *SSL cert* which is imported using the syntax **ca-cert** *file_options3*. ACOS uses SSL certs and private keys to create proxied signed certificates for handshaking with SSL clients. SSL certs are self-signed by a private organization acting as their own CA. The organization configures its SSL clients to accept its CA. See **ca-cert** *file_options3* for information on *file_options3*.
cert-key *file_options4*	Imports a certificate and key together as a single file. **Syntax:** **cert-key bulk** [pfx-password *pswd*] [**user-tag** *user-tag-name*] [**overwrite**] **[use-mgmt-port]** {*url* | *import-store-name* | **terminal}** **Parameters:**

Parameter	Description
	• Use the **bulk** option to import multiple files simultaneously as a .tgz archive. • Use pfx-password *pswd* to specify the PFX certificated password if and only if the certificate type is **pfx**. • **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. The **overwrite** option enables the overwriting of an existing cert-key bulk file. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See url below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
class-list *file_options1*	Import an IP class list. For the *file_options1* syntax, see **aflex** *file_options1*.
class-list-convert *file_options5*	ACOS imports a newline delimited text file and converts it to a class-list file of the specified type: **Syntax:** **class-list-convert** *filename* class-list-type {ac | string |ipv4 | ipv6 | string-case-intensive} [**user-tag** *user-tag-name*] [**proxy** *host:port*] [**overwrite**] [use-mgmt-port] {*url* | *import-store-name* | **terminal**} **Parameters:** • *filename* – local file name. (1 - 63 characters)

Parameter	Description
	• `class-list-type` - type of class list: • **`ac`** - Aho-Corasick class list. See the "How to Convert Your SNI List to an A10 Class List" section in the *SSL Insight* book for an example of converting to an A10 Aho-Corasick class list. • *`string`* - string class list • **`ipv4`** - ipv4 class list • **`ipv6`** - ipv6 class list • **`string-case-insensitive`** - string case insensitive class list **NOTE:** Only the Aho-Corasick class list is compliant with the class list types created through the `class-list` command. • **`user-tag`** *`user-tag-name`* - Custom tag that can then be searched by using the aXAPI. • **`proxy`** *`host:port`* - Specifies explicit HTTP proxy settings for downloading the class list file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *`[a:b::1]:8080`*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **`overwrite`** - Enables the overwriting of an existing file of the same local name. • **`use-mgmt-port`** – See use-mgmt-port below. • *`url`* – See *url* below.

Parameter	Description
	• *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
crl *file_options1*	Import an SSL certificate revocation list (CRL). For the *file_options1* syntax, see **aflex** *file_options1*. The CRL file name can be from 1 to 255 characters. **NOTE:** When traffic is flowing, the process of loading a large CRL file will consume a significant amount of time. It is recommended to load large CRL files before the initiation of traffic or during maintenance periods. Additionally, frequent updates of large CRL files should be avoided.
dnssec-dnskey *file_options1*	Import a DNSEC key-signing key (KSK) file. For the *file_options1* syntax, see **aflex** *file_options1*. The DNSSEC DNSKEY (KSK) file name can be from 1 to 127 characters.
dnssec-ds *file_options1*	Import a DNSSEC DS file. For the *file_options1* syntax, see **aflex** *file_options1*. The DNSSEC DS file name can be from 1 to 127 characters.
file-inspection-bw-list *file_options1*	Import a Cylance black and white list from Cylance which lists files that were determined to either be good or bad through additional qualification means outside the Cylance machine learning algorithm. **Syntax:** **file-inspection-bw-list** [use-mgmt-port]

Parameter	Description
	Parameters: **use-mgmt-port** - See use-mgmt-port below.
geo-location *file_options1*	Imports a geo-location data file for Global Server Load Balancing (GSLB). For the *file_options1* syntax, see **aflex** *file_options1*.
glm-cert *file_options1*	Imports an global license manager (GLM) certificate. For the *file_options1* syntax, see **aflex** *file_options1*.
glm-license *file_options1*	Imports an activation key license file provided by the global license manager (GLM). For the *file_options1* syntax, see **aflex** *file_options1*.
health-external *file_options6*	Import an external health monitor program. Importing external health monitor scripts is only supported for administrative users provisioned with health monitor (hm) privilege. If commands with this parameter fail due to insufficient privilege, contact your ACOS root administrator. For more information, see the *Application Delivery and Server Load Balancing Guide* (*Using External Health Methods* section) and the *Management Access and Security Guide*. **Syntax:** **health-external** *program-name* **[description** *function*] [proxy host:port] **overwrite**] [use-mgmt-port] *url* **Parameters:**

Parameter	Description
	• *program-name* – local health monitor program name. (1 - 31 characters) • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the external health monitor file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, [a:b::1]:8080 ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - Enables the overwriting of an existing program of the same local name • Use the **description** *function* option to provide a brief description (1-63 characters) of the program purpose or function. • **use-mgmt-port** – See use-mgmt-port below. *url* – See *url* below. **Security Notes:** External health monitors run on a system-level basis at escalated privilege within the ACOS, independent of partition-level constraints. Importing their underlying scripts represents an avenue for potentially malicious code to be introduced into the ACOS system which could be used to compromise the security of the ACOS system or its connected environment. To better ensure confidentiality, integrity, and

Parameter	Description
	availability in an ACOS installation, external health monitor scripts should be carefully reviewed and audited to verify their contents are for the intended monitoring purpose and are free of unsanctioned or untrusted code.
health-postfile *file_options7*	Import the health monitor HTTP post data file. **Syntax**: **health-postfile** *filename* **[proxy** *host:port***]** **[overwrite]** **[use-mgmt-port]** *url* **Parameters**: • *filename* – local health monitor HTTP post data filename. (1 - 31 characters) • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the HTTP post data file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - Enables the overwriting of an existing file of the same local name • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below.
ip-map-list *file_options1*	IP Map List file For the *file_options1* syntax, see **aflex** *file_options1*

Parameter	Description
key *file_options8*	Import the SSL key file. **Syntax:** **key {bulk |** *filename*} [**user-tag** *user-tag-name*] [**overwrite**] [use-mgmt-port] {*url* | *import-store-name* | **terminal}** **Parameters:** • Use the **bulk** option to import multiple files simultaneously as a .tgz archive. • *filename* - local file name (1-255 alphanumeric characters) • **user-tag** *user-tag-name* - Custom tag that can then be searched by using the aXAPI. • The **overwrite** option enables the overwriting of an existing file of the same local name • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. • *import-store-name* - Name of a file stored on ACOS drive memory. • **terminal** - Terminal vi operation.
local-uri-file *file_options1*	Import the local URI files for HTTP responses. For the *file_options1* syntax, see **aflex** *file_options1*
lw-4o6 *file_options1*	Import the LW-4over6 binding table file. For the *file_options1* syntax, see **aflex** *file_options1*
ng-waf-custom-page *html_file*	Import the custom HTML file for Next Generation WAF (NGWAF). **Syntax:**

Parameter	Description
	ng-waf-custom-page *html_file* **{[proxy** *host:port* **] | [overwrite] | [use-mgmt-port]{***url***} }** **Parameters:** • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the HTML file. The parameter supports using IPv4, IPv6, or hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080* ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** - option enables overwriting the existing file of the same local name. • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. **NOTE**: The HTML file size should not exceed 100 KB.
ng-waf-module	Import the Next Generation WAF (NGWAF) module. **Syntax:** **ng-waf-module {[proxy** *host:port***] | [overwrite] | [use-mgmt-port]{***url***} }** **Parameters:** • **proxy** *host:port* - Specifies explicit HTTP proxy settings for downloading the NGWAF module. The parameter supports using IPv4, IPv6, or

Parameter	Description
	hostname along with the proxy port number. **NOTE:** ◦ An IPv6 address must be encased in a bracket, for example, *[a:b::1]:8080*. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • **overwrite** • **use-mgmt-port** – See use-mgmt-port below. • *url* – See *url* below. **NOTE**: The NG-WAF module can be downloaded only from the following url, https://dl.signalsciences.net/sigsci-agent/sigsci-agent_latest.tar.gz
rzp	Refer to import rpz for details.
tsig*file_ options1*	Import the Trasaction Signature (TSIG) key file. The key can be private or public. **Syntax:** **tsig** *filename* {[**user-tag** *user-tag-name*] [**overwrite**] [**use-mgmt-port**] {*url* | *import-store-name* }**}** **Parameters:** • *filename* – local file name (1-63 characters) • **user-tag** *user-tag-name* – Custom tag that can then be searched by using the aXAPI. • The **overwrite** option enables overwriting the existing file of the same local name • **use-mgmt-port** – See use-mgmt-port below.

Parameter	Description
	• *url* – See *url* below. • *import-store-name*- Name of a file stored on ACOS drive memory.
store *file_options9*	Import a storage name for a remote URL. • **store {create** *profile-name url* **| delete** *profile-name***}** • Use **create** to create an import store profile • Use **delete** to delete an import store profile • *profile-name* – name of the ACOS profile to store the remote URL (1 - 31 characters) • *url* – See *url* below.
thales-secworld *file_options1*	Import a Thales security world file. For the *file_options1* syntax, see **aflex** *file_options1*
usb-license *file_options1*	Imports an activation key license file provided from a USB Key. For the *file_options1* syntax, see **aflex** *file_options1*.
web-category-license *file_options1*	Import a web-category-license file, which is required if you wish to access the BrightCloud server and use the web-categorization feature. For the *file_options1* syntax, see **aflex** *file_options1*
wsdl *file_options1*	Import a WSDL file. For the *file_options1* syntax, see **aflex** *file_options1*
xml-schema *file_options1*	Import an XML schema file. For the *file_options1* syntax, see **aflex** *file_*

Parameter	Description
	options1
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	Protocol, user name (if required), and directory path you want to use to send the file. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. The following special characters are supported: • **tftp** - No password required • **ftp** - `!#$%()*+,.: []^_`\|~=` • **scp** - `!#$%()*+,-.:;[]^_`{}|~=` • **http** - `!$%()*+,-.: []^_`{}\|~=` • **https** - `!$%()*+,-.: []^_`{}|~=` • **sftp** - `!#$()*+,-.;=^_`{|}~[]`  The following special characters are not supported:  • **tftp** - No password required • **scp** - All are supported • **ftp** - `-;{}` • **http** - `#;`

Parameter	Description
	• **https** - #; • **sftp** - %: **Syntax:** **{** **tftp://***host/file* **|** **ftp://[***user@***]***host*[:*port*]**/***file* **|** **scp://[***user@***]***host/file* **|** **http://[***user@***]***host/file* **|** **https://[***user@***]***host/file* **|** **sftp://[***user@***]***host/file* **|** **}** **Parameters:** *file* - remote file name **NOTE:** • This command can be executed only in the shared partition. • In case of **http/https** URL, you must replace ? with %3F. For example: For **import geo-location aa use-mgmt-port** https://geoblocklist.com/getblocklist.php **?**licenseKey=T3GVxx1Y use **import geo-location aa use-mgmt-port** https://geoblocklist.com/getblocklist.php **%3F**licenseKey=T3GVxx1Y

Syntax Privileged EXEC mode or global configuration mode

Example The following command imports an aFleX policy onto the ACOS device from a TFTP server, from its directory named “backups”:

```
ACOS# import aflex aflex-01
tftp://192.168.1.101/backups/aflex-01
```

Example The following command imports an RPZ file onto the ACOS device:

```
ACOS# import rpz A10.rpz use-mgmt-port
scp://root@192.168.93.182/root/A10.rpz
```

Example The following command imports an NGWAF agent:

```
ACOS# import ng-waf-module
https://dl.signalsciences.net/sigsci-agent/sigsci-agent_
latest.tar.gz
```

Example The following command imports an NGWAF agent using HTTP proxy settings:

```
ACOS(config)# import ng-waf-module proxy [2001:db8::1]:3128
https://dl.signalsciences.net/sigsci-agent/sigsci-agent_
latest.tar.gz
```

Example The following command imports a custom HTML page for NGWAF:

```
ACOS# import ng-waf-custom-page mypage
scp://hostname@192.168.1.101/ngwaf/index.html
```

Example The following command imports a custom HTML page for NGWAF using HTTP proxy settings:

```
ACOS(config)# import ng-waf-custom-page mypage proxy
myproxy.com:443 https://www.google.com
```

Example The following command imports the TSIG private key file:

```
ACOS# import tsig Krpz.com.+157+20696.private use-mgmt-port
scp://root@192.168.93.182/root/Krpz.com.+157+20696.private
```

Example The following command imports a JSON web key file:

```
ACOS# import auth-jwks jwks_file
scp://root@192.168.93.182/root/jwks_file
```

import-periodic

Description Get files from a remote site periodically.

When the `import-periodic` command is used on the Multi-PU platforms, the imported files are automatically synced from PU1 to PU2, ensuring that PU2 can periodically and locally update the files. This also helps both PU1 and PU2 to import the same files.

Syntax

```
import-periodic file-type options
```

Parameter	Description
aflex *file_options1*	Imports an aFleX file.
auth-jwks *file_options1*	Imports a JSON web key file for Application Access Management (AAM).
auth-portal *file_options1*	Imports an authentication portal file for Application Access Management (AAM).
bw-list *file_options1*	Imports a black/white list.
class-list *file_options1*	Imports an IP class list.
class-list-convert *file_options3*	ACOS imports a newline delimited text file and converts it to a class-list file of the type specified by `class-list-type`.
dnssec-dnskey *file_options1*	Imports a DNSEC key-signing key (KSK) file.
dnssec-ds *file_options1*	Imports a DNSSEC DS file.
file-inspection-bw-list *file_options2*	Imports a Cylance black and white list from Cylance.
geo-location *file_options1*	Imports a geo-location data file for Global Server Load Balancing (GSLB).
glm-license *file_options1*	Imports an activation key license file provided by the global license manager (GLM).

Parameter	Description
ip-map-list *file_options1*	IP Map List file
local-uri-file *file_options1*	Imports a local URI file.
rpz *file_options1*	Imports an Response Policy Zone (rpz) file.
ssl-cert *file_options4*	Imports an SSL certificate.
ssl-cert-key *file_options5*	Imports an SSL certificate and key together as a single .tgz file.
ssl-crl *file_options6*	Imports an SSL key.
ssl-key *file_options7*	Import a certificate revocation list (CRL).
thales-kmdata *file_options8*	Imports Thales KMdata files in .tgz format
thales-secworld *file_options8*	Import Thales Security World files in .tgz format.
wsdl *file_options1*	Imports a WSDL file.
xml-schema *file_options1*	Imports an XML schema file.

Parameter Option	Parameter Option Description and Syntax
file_options1	**Syntax:** *filename* [use-mgmt-port] *url* **period** *seconds* **Syntax Parameters** • *filename* – local file name. • use-mgmt-port • *url*

Parameter Option	Parameter Option Description and Syntax
	• period seconds
file_ options2	**Syntax:** `[use-mgmt-port] url` **`period`** *`seconds`* **Syntax Parameters** • use-mgmt-port • period seconds
file_ options3	**Syntax:** **`class-list-convert`** *`filename`* `class-list-type {ac | string |ipv4 | ipv6 | string-case-intensive} [use-mgmt-port] url` **`period`** *`seconds`* **Syntax Parameters:** • *`filename`* – local file name. • `class-list-type` - type of class list: **`ac`** - Aho-Corasick class list. For more information, see "How to Convert Your SNI List to an A10 Class List" section in the *SSL Insight* book for an example of converting to an A10 Aho-Corasick class list. *`string`* - string class list **`ipv4`** - ipv4 class list **`ipv6`** - ipv6 class list **`string-case-insensitive`** - string case insensitive class list **NOTE:** Only the Aho-Corasick class list is compliant with the class list types created through the `class-list` command.

Parameter Option	Parameter Option Description and Syntax
	• use-mgmt-port • *url* • period seconds
file_ options4	**Syntax:** **ssl-cert {bulk |** *filename*} [**certificate-type** {**pem** | **der** | **pfx** | **p7b**}] [*pswd*] **[use-mgmt-port]** *url* **period** *seconds* **Syntax Parameters:** • Use the **bulk** option to import multiple files simultaneously as a .tgz archive. • *filename* – local file name. • Use **certificate-type** {**pem** | **der** | **pfx** | **p7b**} to specify a certificate type. • Use *pswd* to specify the PFX certificated password if you have specified the **pfx** certificate type. • use-mgmt-port • *url* • period seconds
file_ options5	**Syntax:** **ssl-cert-key bulk [use-mgmt-port]** *url* **period** *seconds* **Syntax Parameters:** The **bulk** keyword imports a .tgz archive. • use-mgmt-port • *url* • period seconds

Parameter Option	Parameter Option Description and Syntax
file_ options6	**Syntax:** **ssl-crl** *filename* **[use-mgmt-port]** *url* **period** *seconds* **Syntax Parameters:** • *filename* – local file name. • use-mgmt-port • *url* • period seconds
file_ options7	**Syntax:** **ssl-key {bulk |** *filename*} **[use-mgmt-port]** *url* **period** *seconds* **Syntax Parameters:** The **bulk** keyword imports a .tgz archive containing the ssl-key file. • *filename* – local file name. • use-mgmt-port • *url* • period seconds
file_ options8	**Syntax:** **thales-kmdata** *filename* **[overwrite]** [use-mgmt-port] *url* **period** *seconds* **Syntax Parameters:** • *filename* – local file name. The **overwrite** option enables the overwriting of existing Thales KMdata files of the same local name

Parameter Option	Parameter Option Description and Syntax
	• use-mgmt-port • *url* • period seconds
url	Protocol, user name (if required), and directory path you want to use to send the file. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. The following special characters are supported: • **tftp** - No password required • **ftp** - !#$%()*+,.: []^_`\|~= • **scp** - !#$%()*+,-.:;[]^_`{}|~= • **http** - !$%()*+,-.: []^_`{}\|~= • **https** - !$%()*+,-.: []^_`{}|~= • **sftp** - !#$()*+,-.;=^_`{|}~[] The following special characters are not supported: • **tftp** - No password required • **scp** - All are supported • **ftp** - -;{} • **http** - #; • **https** - #; • **sftp** - %: **Syntax:**

Parameter Option	Parameter Option Description and Syntax
	{ **tftp://***host*/*file* **|** **ftp://[***user***@]***host***[:***port***]/***file* **|** **scp://[***user***@]***host*/*file* **|** **http://[***user***@]***host*/*file* **|** **https://[***user***@]***host*/*file* **|** **sftp://[***user***@]***host*/*file* **|** **}** **Syntax Parameters:** *file* – remote file name
period *seconds*	Enables periodic update of imported files automatically. You can specify 60-31536000 seconds. The periodic update occurs at the multiple of 60 seconds intervals even when the value specified is not in the multiple of 60 seconds. For example, if you set the period option to 90 seconds, the import interval automatically sets to 120 seconds. Similarly, if you set the period option to 150 seconds, the import interval automatically sets to 180 seconds. The **period** option simplifies update of imported files, especially files that are used by multiple ACOS devices. You can edit a single instance of the file, on the remote server, then configure each of ACOS device to automatically update the file to import the latest changes. When you use this option, the ACOS device periodically replaces the specified file with the version that is currently on the remote server. If the file is in use in the running-config, the updated version of the file is placed into memory.

Parameter Option	Parameter Option Description and Syntax
	The updated file affects only new sessions that begin after the update but does not affect existing sessions. For example, when an aFleX script that is bound to a virtual port is updated, the update affects new sessions that begin after the update, but does not affect existing sessions that began before the update.
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.

Mode Privileged EXEC mode or global configuration mode

Example The following command imports an aFleX policy onto the ACOS device from a TFTP server, from its directory named “backups” every 30 days:

```
ACOS(config)# import-periodic aflex aflex-01
tftp://192.168.1.101/backups/aflex-01 period 2592000
```

import-periodic geo-location

Description Get files from a remote site periodically.

Syntax

```
import-periodic geo-location [use-mgmt-port] {<db_name> |
<name> | {tftp:| ftp: | scp: | http: | https: | sftp:
<[user@]hostname/filename>} period <seconds>
```

Parameter	Description
geo-location	IPv4 or IPv6 address of the device you want to test.
<*db_name*>	User-defined database name loaded on ACOS.
<*name*>	Geo-location CSV filename of length from 1 to 63.
use-mgmt-port	Use management port as source port

Parameter	Description
tftp:	Remote file path of tftp: file system (Format: tftp://host/file)
ftp:	Remote file path of ftp: file system (Format:ftp://[user@]host[:port]/file)
scp:	Remote file path of scp: file system (Format:scp://[user@]host/file)
http:	Remote file path of http: file system (Format:http://[user@]host/file)
https:	Remote file path of https: file system (Format:https://[user@]host/file)
sftp:	Remote file path of sftp: file system (Format:sftp://[user@]host/file)
period	Time in seconds.

Mode Configuration Mode

Usage Once the geo-location list is imported, it can be used in firewall rule-set.

Example

```
ACOS(config)# import-periodic geo-location USER_DB use-mgmt-port tftp://host/user_db.csv period 1200
```

import rpz

Description Import the Response Policy Zone (rpz) files from a remote site using the specified protocol.

Syntax

```
import rpz rpz_name { zone-transfer | user-tag user-tag-name | overwrite | use-mgmt-port | url | import-store-name }
```

Parameter	Description
rpz_name	Enter the file name (1-63 characters).
overwrite	Specify this option to overwrite the existing RPZ file of the same local name.

Parameter	Description
use-mgmt-port	Specify this option to use the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. If this option is not specified, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
user-tag*user-tag-name*	Specify this option along with the custom tag that can be searched using the aXAPI.
zone-transfer { **overwrite** | **use-mgmt-port** | **user-tag** *user-tage-name* | **axfr:** *file* | *import-store-name* }	Specify this option to enable zone transfer. The following sub-options can be configured: **overwrite** - Refer to overwrite. **use-mgmt-port** - Refer to use-mgmt-port. **user-tag** - Refer to user-taguser-tag-name. **axfr** - Use this option to transfer the RPZ file using the standard full zone transfer (AXFR) protocol. Specify the RPZ file along with the Transaction Signature (TSIG) key file in the following format: **axfr:***//[tsig-keyfile@]host/domain-name)* The TSIG public key, as well as private key, must be present on the system while importing an RPZ file using AXFR protocol.
url	Specify the protocol, username (if required), and directory path to send the file. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and

Parameter	Description
	a password is required, you will still be prompted for the password. The password can be up to 255 characters long. The following URL options can be configured: *{ tftp://host/file* *| ftp://[user@]host[:port]/file* *| scp://[user@]host/file* *| http://[user@]host/file* *| https://[user@]host/file* *| sftp://[user@]host/file }* This command can be executed only in the shared partition.
import-store-name	Specify the name of a file stored on the ACOS drive memory.

Mode Privileged EXEC mode or global configuration mode

Usage The file can be fetched using multiple protocols (SCP, SFTP, FTP, TFTP, HTTP, HTTPS) or via DNS AXFR zone transfer.

If the system detects any validation errors in the incoming RPZ file, such as syntax errors, invalid rule types, or exceeding the global rule limit, the entire import is rejected and the existing RPZ remains active.

NOTE:

The command does not work as expected on Multi-PU platforms. The following issues occur:

- On the Shared partition:
  - When an RPZ is imported (non-periodic) using SCP or AXFR, it does not synchronize to PU2.
  - When an RPZ is imported (periodically) using SCP or AXFR, only the initial import synchronizes to PU2; subsequent periodic imports fail to synchronize.
  - On PU1, issues arise while attaching an RPZ to an SLB template and while deleting an imported RPZ.

  Corresponding error messages are logged for all these issues.
- On an L3V partition:

  All the issues listed for Shared partitions occur on L3V partitions as well. However, error messages are not logged.

Example The following command imports an RPZ file onto the ACOS device using the management port:

```
ACOS# import rpz A10.rpz use-mgmt-port
scp://root@192.168.93.182/root/A10.rpz
```

Example The following command imports an RPZ file onto the ACOS device using zone transfer with TGIS:

```
ACOS# import rpz test.rpz zone-transfer use-mgmt-port
axfr://Krpz.com.+157+20696.key@192.168.93.182/rpz.com
```

ip-list

Description Create a list of IP addresses with group IDs to be used by other GSLB commands.

For example, you can create an IP list and use it in a GSLB policy.

Refer to *Global Server Load Balancing Guide* for more information.

Syntax

```
[no] ip-list list-name
```

After entering this command, you are placed in a sub-configuration mode where you can enter the IP addresses as follows:

```
ipv4-addr [to  end-ipv-addr]
ipv6-addr [to  end-ipv6-addr]
ipv6-addr/range [count  num] [to  end-ipv6-addr/range]
```

Mode Configuration mode

Example The following example shows how to use the **ip-list** command to create a list of IPv4 addresses from 10.10.10.1 to 10.10.10.44:

```
ACOS(config)# ip-list ipv4-list
ACOS(config-ip-list)# 10.10.10.1 to 10.10.10.44
```

l2-bfd

Description Configure the global-level layer 2 health monitoring feature using layer 2 BFD.

Syntax

```
[no] l2-bfd {ether-type | rx-interval | tx-interval | multiplier}
```

Parameter	Description
ether-type *<1-4>*	Specify the ethernet payload type for layer 2 BFD packets. The value should be 16 bits hex. By default, the value is set to 88B6.
rx-interval *<48-1000>*	Specify the minimum amount of time (in milliseconds) that the ACOS device waits to receive a BFD control packet from a BFD neighbor. If a control packet is not received within the specified time, the multiplier (below) is incremented by 1. The value can be between 48-1000 milliseconds. By default, the value is set to 800.
tx-interval	Specify the transmit interval (in milliseconds) between BFD packets.

Parameter	Description
<48-1000>	The value can be between 48-1000 milliseconds. By default, the value is set to 800.
multiplier <3-50>	Specify the maximum number of consecutive times the ACOS device will wait for a BFD control packet from a neighbor. If the multiplier value is reached, the ACOS device concludes that the routing process on the neighbor is down. The value can be between 3-50. By default, the value is set to 4.

Default As mentioned in the table

Mode Global Configuration mode

Usage The layer 2 BFD is utilized to provide a fast forwarding path failure detection for layer 2 health monitoring.

This is the global-level setting for enabling layer 2 health monitoring feature. You can also configure **l2-bfd** at the individual health-monitor level (see **system health-check**). However, the global setting reduces the overall configuration size by abstracting the common settings and overriding the individual setting.

Example The following command sets the layer 2 health monitoring settings:

```
ACOS(config)# l2-bfd
ACOS(config-l2-bfd)# ether-type 88B6
ACOS(config-l2-bfd)# rx-interval 50
ACOS(config-l2-bfd)# tx-interval 50
ACOS(config-l2-bfd)# multiplier 3
```

Related Commands:

- system health-check
- system path

l3-vlan-fwd-disable

Description Globally disable Layer 3 forwarding between VLANs.

Syntax

```
[no] l3-vlan-fwd-disable
```

Default By default, the ACOS device can forward Layer 3 traffic between VLANs.

Mode Configuration mode

Usage This command is applicable only on ACOS devices deployed in gateway (route) mode. If the option to disable Layer 3 forwarding between VLANs is configured at any level, the ACOS device can not be changed from gateway mode to transparent mode, until the option is removed.

Depending on the granularity of control required for your deployment, you can disable Layer 3 forwarding between VLANs at any of the following configuration levels:

- Global – Layer 3 forwarding between VLANs is disabled globally, for all VLANs, on ACOS devices deployed in gateway mode. (Use this command at the Configuration mode level.)
- Individual interfaces – Layer 3 forwarding between VLANs is disabled for incoming traffic on specific interfaces.
- Access Control Lists (ACLs) – Layer 3 forwarding between VLANs is disabled for all traffic that matches ACL rules that use the **l3-vlan-fwd-disable** action.

The show slb switch is used to display statistics for this option.

Related Commands:

- l3-vlan-fwd-disable
- access-list (standard)
- access-list (extended)

lacp system-priority

Description Set the Link Aggregation Control Protocol (LACP) priority.

Syntax

```
[no] lacp system-priority num
```

Replace *num* with the LACP system priority, 1-65535. A low priority number indicates a high priority value. The highest priority is 1 and the lowest priority is 65535.

Default 32768

Mode Configuration mode

Usage In cases where LACP settings on the local device (the ACOS device) and the remote device at the other end of the link differ, the settings on the device with the higher priority are used.

lacp-passthrough

Description Specify peer ports to which received LACP packets can be forwarded.

Syntax

```
lacp-passthrough ethernet fwd-port  ethernet  rcv-port
```

Parameter	Description
fwd-port	Peer member that will forward LACP packets.
rcv-port	Peer member that will receive the forwarded LACP packets.

Default Not set

Mode Configuration mode

ldap-server

Description Set Lightweight Directory Access Protocol (LDAP) parameters for authenticating administrative access to the ACOS device.

Syntax

```
[no] ldap-server host
{hostname | ipaddr}
{cncn-namedndn-name |
  domaindomain-name [basebase-domain] [groupgroup-id]}
[portportnum]
[ssl]
[timeoutseconds]
```

Parameter	Description
hostname	Host name of the LDAP server.
ipaddr	IP address of the LDAP Server.
cn-name	Value for the Common Name (CN) attribute.

dn-name	Value for the Distinguished Name (DN) attribute.
	
	The DN attribute does not support spaces or quotation marks. For example, the following DN string syntax is valid:
	
	`cn=xxx3,dc=maxcrc,dc=com`
	
	The following string *is not* valid because of the quotation marks and space character:
	
	`"cn=xxx3,dc=max crc,dc=com"`

domain-name	Active Directory domain name.
base-domain	Base domain to which the user belongs.
group-id	Group ID to which the user belongs.
portnum	Protocol port on which the server listens for LDAP traffic. The default is 389.
seconds	Maximum number of seconds the ACOS device waits for a reply from the LDAP server for a given request (1-60 seconds). If the LDAP server does not reply before the timeout, authentication of the admin fails. The default is 44 seconds.
`ssl`	Authenticate using SSL.

Default No LDAP servers are configured by default. When you add an LDAP server, it has the default settings described in the table above.

Mode Configuration mode

Usage This command can also be run in L3V partitions, so that each L3V partition can have its own independent LDAP server for authentication.

For more information, see "Lightweight Directory Access Protocol" chapter of the *Management Access and Security Guide*.

Example The following commands enable LDAP authentication and add LDAP server 192.168.101.24:

```
ACOS(config)# authentication type ldap
ACOS(config)# ldap-server host 192.168.101.24 cn cn dn
ou=UserAccount,dc=example,dc=com
```

link

Description Link the "startup-config" token to the specified configuration profile. By default, "startup-config" is linked to "default", which means the configuration profile stored in the image area from which the ACOS device most recently rebooted.

Syntax

```
link startup-config {default | profile-name} [primary |
secondary]
```

Parameter	Description
default	Links "startup-config" to the configuration profile stored in the image area from which the ACOS device was most recently rebooted.
profile-name	Links "startup-config" to the specified configuration profile.
primary | **secondary**	Specifies the image area. If you omit this option, the image area last used to boot is selected.

Default The "startup-config" token is linked to the configuration profile stored in the image area from which the ACOS device was most recently rebooted.

Mode Configuration mode

Usage This command enables you to easily test new configurations without replacing the configuration stored in the image area.

The profile you link to must be stored on the boot device you select. For example, if you use the default boot device (hard disk) selection, the profile you link to must be stored on the hard disk. If you specify cf, the profile must be stored on the compact flash. (To display the profiles stored on the boot devices, use the show startup-config command.)

After you link "startup-config" to a different configuration profile, configuration management commands that affect "startup-config" affect the linked profile instead of affecting the configuration stored in the image area. For example, if you enter the **write memory** command without specifying a profile name, the command saves the running-config to the linked profile instead of saving it to the configuration stored in the image area.

Likewise, the next time the ACOS device is rebooted, the linked configuration profile is loaded instead of the configuration that is in the image area.

To relink "startup-config" to the configuration profile stored in the image area, use the default option (**link startup-config default**).

Example The following command links configuration profile "slbconfig3" with "startup-config":

```
ACOS(config)# link startup-config slbconfig3
```

Example The following command relinks "startup-config" to the configuration profile stored in the image area from which the ACOS device was most recently rebooted":

```
ACOS(config)# link startup-config default
```

lldp

lldp enable

Description Use this command to enable or disable LLDP from the global level. You can enable LLDP to either receive only, transmit only, or transmit and receive.

Syntax

```
lldp enable [rx] [tx]

no lldp enable
```

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example To enable LLDP transmission and receipt from the global level, issue the following command:

```
ACOS(config)# lldp enable rx tx
```

lldp management-address

Description Configures the management-address that can include the following information:

- DNS name
- IPv4 address
- IPv6 address

Optionally, you can specify the interface on which the management address is configured. The management interface can be either a physical Ethernet interface or a virtual interface (VE).

Syntax

```
[no] lldp management-address
  {dns dns-value | ipv4 ipv4-value ipv6 ipv6-value}
    interface {ethernet eth-num | management | ve ve-num}
```

Default Not set

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

lldp notification interval

Description This object controls the interval between transmission of LLDP notifications during normal transmission periods.

Syntax

```
[no] lldp notification interval notification-value
```

Default 30

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

lldp system-description

Description Defines the alpha-numeric string that describes the system in the network.

Syntax

```
[no] lldp system-description sys-description-value
```

Default None

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

lldp system-name

Description Defines the string that will be assigned as the system name.

Syntax

```
[no] lldp system-name system-name-value
```

Default hostname

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example The following command will set the LLDP system name to “testsystem”:

```
ACOS(config)# lldp system-name testsystem
```

lldp tx fast-count

Description This value is used as the initial value for the Fast transmission variable. This value determines the number of LLDP data packets that are transmitted during a fast transmission period. This value can range from 1-8 seconds.

Syntax

```
[no] lldp tx fast-count value
```

Default 4

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example The following command will set the LLDP fast count transmission value to 3 seconds:

```
ACOS(config)# lldp tx fast-count 3
```

lldp tx fast-interval

Description This variable defines the time interval in timer ticks between transmissions during fast transmission periods (that is, txFast is non-zero). The range for this variable is 1-3600 seconds.

Syntax

```
[no] lldp tx fast-interval
```

Default 1 second

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example The following command will set the LLDP fast transmission interval value to 2000 seconds:

```
ACOS(config)# lldp tx fast-interval 2000
```

lldp tx hold

Description Determines the value of the message transmission time to live (TTL) interval that is carried in LLDP frames. The hold-value can be from 1 to 100 seconds.

Syntax

```
[no] lldp tx hold hold-value
```

Default Default 4 seconds

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example The following command will set the transmission hold time to 255:

```
ACOS(config)# lldp tx hold 255
```

lldp tx interval

Description Defines the transmission (tx) interval between a normal transmission period.

Syntax

```
[no] lldp tx interval value
```

Replace *value* with the transmission interval from 1 to 3600 seconds.

Default 30 seconds

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example The following command will set the transmission interval to 200:

```
ACOS(config)# lldp tx interval 200
```

lldp tx reinit-delay

Description Indicates the delay interval when the administrative status indicates 'disabled' after which re-initialization is attempted. The range for the *reinit-delay-value* is 1-5 seconds.

Syntax

```
[no] lldp tx reinit-delay reinit-delay-value
```

Default 2 seconds

Mode Configuration mode

Usage LLDP commands are only available in the shared partition.

Example The following command will set the retransmission delay to 3 seconds:

```
ACOS(config)# lldp tx reinit-delay 3
```

locale

Description Set the CLI locale.

Syntax

```
[no] locale {test | locale}
```

Default en_US.UTF-8

Mode Configuration mode

Usage Use this command to configure the locale or to test the supported locales.

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the Multi-PU platforms to which to apply this command.

Example The following commands test the Chinese locales and set the locale to zh_CN.GB2312:

```
ACOS(config)# locale test zh_CN
ACOS(config)# locale zh_CN.GB2312
```

logging

logging auditlog host

Description Configure audit logging to an external server.

Syntax

```
[no] logging auditlog host {ipaddr | hostname}
[facility facility-name][port num]]
```

Parameter	Description
ipaddr	IP address of the remote server.
hostname	Host name of the remote server.
facility-name	Name of a log facility: • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **local7** There is no default.

Parameter	Description
port num	Specify the remote audit log port number of the remote server.

Default N/A

Mode Configuration mode

Usage The audit log is automatically included in system log backups. You do not need this command in order to back up audit logs that are within the system log.

In the current release, only a single log server is supported for remote audit logging.

Related Commands:

- backup system
- backup log

logging buffered

Description Configure the event log on the ACOS device.

Syntax

```
[no] logging buffered max-messages
```

Syntax

```
[no] logging buffered
{disable | emergency | alert | critical | error | warning |
notification | information | debugging}
```

Parameter	Description
max-messages	Specifies the maximum number of messages the event log buffer will hold. The default buffer size (maximum messages) is 30000.
disable	Disable logging to the monitor.
emergency	Send emergency events (severity level 0—system unusable) to the monitor.
alert	Send alert events (severity level 1—take action immediately) to the monitor.

Parameter	Description
critical	Send critical events (severity level 2—system is in critical condition) to the monitor.
error	Send error events (severity level 3—system has an error condition) to the monitor.
warning	Send warning events (severity level 4—system has warning conditions) to the monitor.
notification	Send notifications (severity level 5—normal but significant conditions) to the monitor.
information	Send informational messages (severity level 6) to the monitor.
debugging	Send debug level messages (severity level 7) to the monitor.

Mode Configuration mode

Example The following command sets the severity level for log messages to 7 (debugging):

```
ACOS(config)# logging buffered debugging
```

logging console

Description Set the logging level for messages sent to the console.

Syntax

```
[no] logging console
{disable | emergency | alert | critical | error | warning |
 notification | information | debugging}
```

Parameter	Description
disable	Disable logging to the console.
emergency	Send emergency events (severity level 0—system unusable) to the console.
alert	Send alert events (severity level 1—take action immediately) to the console.
critical	Send critical events (severity level 2—system is in

Parameter	Description
	critical condition) to the console.
error	Send error events (severity level 3—system has an error condition) to the console.
warning	Send warning events (severity level 4—system has warning conditions) to the console.
notification	Send notifications (severity level 5—normal but significant conditions) to the console.
information	Send informational messages (severity level 6) to the console.
debugging	Send debug level messages (severity level 7) to the console.

Default Level 3—Error messages

Mode Global configuration

logging disable-partition-name

Description Disable display of L3V partition names in log messages.

Syntax

```
[no] logging disable-partition-name
```

Default Display of L3V partition names in log messages is enabled by default.

Mode Configuration mode

Usage When this option is enabled partition names are included in log messages as the following example illustrates.

```
Jan 24 2014 15:30:21 Info    [HMON]:<partition_1> SLB server
rs1 (4.4.4.4) is down
Jan 24 2014 15:30:19 Info    [HMON]:<partition_1> SLB server
rs1 (4.4.4.4) is up
Jan 24 2014 15:30:17 Info    [ACOS]:<partition_1> Server rs1
is created
```

logging email buffer

Description Configure log email settings.

Syntax

```
[no] logging email buffer [number num] [time minutes]
```

Parameter	Description
num	Specifies the maximum number of messages to buffer (16-256). The default number is 50 messages.
minutes	Specifies how long to wait before sending all buffered messages, if the buffer contains fewer than the maximum allowed number of messages. You can specify 10-1440 minutes. The default time is 10 minutes.

Default By default, emailing of log messages is disabled. When you enable the feature, the buffer options have the default values described in the table above.

Mode Configuration mode

Usage To configure the ACOS device to send log messages by email, you also must configure an email filter and specify the email address to which to email the log messages.

Example The following command configures the ACOS device to buffer log messages to be emailed. Messages will be emailed only when the buffer reaches 32 messages, or 30 minutes passes since the previous log message email, whichever happens first.

```
ACOS(config)# logging email buffer number 32 time 30
```

Related Commands:

- logging email filter
- logging email-address

logging email filter

Description Configure a filter for emailing log messages.

Syntax

```
[no] loggingemailfilterfilter-num"conditions"operators
[trigger]
```

Parameter	Description
filter-num	Specify the filter number (1-8).
conditions	Message attributes on which to match. The conditions list can contain one or more of the following: Severity levels of messages to send in email. Specify the severity levels by number or word: • 0 - emergency • 1 - alert • 2 - critical • 3 - error • 4 - warning • 5 - notification • 6 - information • 7 - debugging • Software modules for which to email messages. Messages are emailed only if they come from one of the specified software modules. For a list of module names, enter ? instead of a module name, and press Enter. • Regular expression. Standard regular expression syntax is supported. Only messages that meet the criteria of the regular expression will be emailed. The regular expression can be a simple text string or a more complex expression using standard regular expression logic.
operators	Set of Boolean operators (AND, OR, NOT) that specify how the conditions should be compared. The CLI Boolean expression syntax is based on Reverse Polish Notation (also called Postfix Notation), a notation method that places an operator (AND, OR,

Parameter	Description
	NOT) after all of its operands (in this case, the conditions list). After listing all the conditions, specify the Boolean operator(s). The following operators are supported: • AND – All conditions must match in order for a log message to be emailed. • OR – Any one or more of the conditions must match in order for a log message to be emailed. • NOT – A log message is emailed only if it does not match the conditions For more information, see http://en.wikipedia.org/wiki/Reverse_Polish_notation for Reverse Polish Notation
`trigger`	Immediately sends the matching messages in an email instead of buffering them. If you omit this option, the messages are buffered based on the logging email buffer settings.

Default Not set. Emailing of log messages is disabled by default.

Mode Configuration mode

Usage To configure the ACOS device to send log messages by email, you also must specify the email address to which to email the log messages.

Below are some additional usage considerations:

- You can configure up to 8 filters. The filters are used in numerical order, starting with filter 1. When a message matches a filter, the message will be emailed based on the buffer settings. No additional filters are used to examine the message.
- A maximum of 8 conditions are supported in a filter.
- The total number of conditions plus the number of Boolean operators supported in a filter is 16.

- The filter requires a valid module name, even if you omit the **module** option.
- For backward compatibility, the following syntax from previous releases is still supported:

  logging email*severity-level*

  The *severity-level* can be one or more of the following (specify either the severity number o r name):

  - 0 - emergency
  - 1 - alert
  - 2 - critical
  - 5 - notification

  The command is treated as a special filter. This filter is placed into effect only if the command syntax shown above is in the configuration. The filter has an implicit trigger option for emergency, alert, and critical messages, to emulate the behavior in previous releases.

Example The following command configures a filter that matches on log messages if they are information-level messages **and** contain the string "abc". The **trigger** option is not used, so the messages will be buffered rather than emailed immediately.

```
ACOS(config)# logging email filter 1 "level information
pattern abc and"
```

The following command reconfigures the filter to immediately email matching messages.

```
ACOS(config)# logging email filter 1 "level information
pattern abc and" trigger
```

Example The following example configures a filter to send email if the log message is generated by the "AFLEX" module and the severity level is "warning":

```
ACOS(config)# logging email filter 1 "level warning module
AFLEX and"
```

Example The following example configures a filter to send email if the log message has the pattern of “disk is full” or the severity level is “critical”:

```
ACOS(config)# logging email filter 2 "pattern disk is full level critical or"
```

Example The following example configures a filter to send email if the log message is generated by (module “SYSTEM” or “ALB”) and (the severity level is “alert” or has pattern of “unexpected error”)

```
ACOS(config)# logging email filter 3 "module SYSTEM module ALB or level alert pattern unexpected error or and"
```

Related Commands:

- logging email-address

logging email-address

Description Specify the email addresses to which to send event messages.

Syntax

```
[no] logging email-address address
```

Parameter	Description
address	Email address to which event message will be sent. To specify multiple Email addresses, use the **logging email-address** command once for each address.

Default None

Mode Configuration mode

Usage To configure the ACOS device to send log messages by email, you also must configure an email filter.

Example The following command sets two email addresses to which to send log messages:

```
ACOS(config)# logging email-address admin1@example.com
ACOS(config)# logging email-address admin2@example.com
```

Related Commands:

- logging email filter

logging export

Description Send the messages that are in the event buffer to an external file server.

Syntax

```
[no] logging export [all] [use-mgmt-port] url
```

Parameter	Description
all	Include system support messages.
use-mgmt-port	Use the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	Saves a backup of the log to a remote server. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]`  To enter the entire URL:  • `tftp://host/file` • `ftp://[user@]host[:port]/file` • `scp://[user@]host/file` • `sftp://[user@]host/file`

Default Not set

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the Multi-PU platforms to which this command must apply.

Example The following example sends the event buffer to an external file server using FTP. The file “event-buffer-messages.txt” will be created on the remote server.

```
ACOS(config)# logging export
ftp://exampleuser@examplehost/event-buffer-messages.txt
```

logging facility

Description Enable logging facilities.

Syntax `[no] logging facility facility-name`

Parameter	Description
facility-name	Name of a log facility: • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **local7**

Default The default facility is **local0**.

Mode Configuration mode

logging host

Description Specify a Syslog server to which to send event messages.

Syntax

```
[no] logging host {
 partition {shared | partition-name} |
 ipv6addr [port protocol-port [tcp]] [use-mgmt-port] |
 {hostname | ipv4addr} [port protocol-port [tcp]] [use-mgmt-
port]
```

Parameter	Description
`partition`	Use the server configured in the specified partition as the preferred syslog server. This enables you to send the logs from one partition to the syslog server of another partition.
ipv6addr	IPv6 address of the syslog server.
hostname	Host name of the IPv4 syslog server.
ipv4addr	IPv4 address of the syslog server.
protocol-port	Protocol port number to which to send messages (1-32767).
`tcp`	Use TCP as the transport protocol.
`use-mgmt-port`	Establish the connection to the Syslog server using the management port.

Default The default protocol port is 514.

Mode Global configuration

Usage When the command includes the **`partition shared`** parameter, logging settings in the shared partition (including rate limits) take precedence over settings in L3V partitions.

Example Multiple log servers can be created by using the `logging host` command once for each server. If you use the command with the same IP address as an existing logging server, it replaces any existing configuration for that existing server.

The following command configures two external log servers. In this example, both servers use the default syslog protocol port, 514, to listen for log messages.

```
ACOS(config)# logging host 10.10.10.1
ACOS(config)# logging host 10.10.10.2
```

When multiple logging hosts through data port are configured, the syslog messages about data plane are balanced among syslog servers.

For more information, see “System Log Messages” chapter in the *System Configuration and Administration Guide*.

logging lsn

Description Specify Large Scale NAT (LSN) log parameters.

Syntax

```
[no] logging lsn quota-exceeded {
ip-based [with-radius-attribute {custom1 custom2 custom3 imei
imsi msisdn}] | pool-based}
```

Parameter	Description
`quota-exceeded`	Specify the LSN quota exceeded log parameter, based on IP or from LSN pool.
`ip-based`	Specify the LSN quota exceeded log based on private IP. This is disabled by default. Optionally, add RADIUS server attributes for logging using `with-radius-attribute` and at least one of the following parameters: • `custom1, custom2, custom3` - Attribute not covered by other options. For more information, see “Customize RADIUS Attributes” in the *Traffic Logging Guide for IPV6 Migration*. • `imei` - International Mobile Equipment Identity (IMEI) attribute. • `imsi` - International Mobile Subscriber Identity (IMSI) attribute. • `msisdn` - Mobile Station International ISDN Number (MSISDN) attribute.
`pool-based`	Specify the LSN quota exceeded log based on the LSN pool. This is enabled by default.

Default Not set

Mode Global configuration

logging monitor

Description Set the logging level for messages sent to the terminal monitor.

Syntax

```
[no] logging monitor
{disable | emergency | alert | critical | error | warning |
 notification | information | debugging}
```

Parameter	Description
disable	Disable logging to the monitor.
emergency	Send emergency events (severity level 0—system unusable) to the monitor.
alert	Send alert events (severity level 1—take action immediately) to the monitor.
critical	Send critical events (severity level 2—system is in critical condition) to the monitor.
error	Send error events (severity level 3—system has an error condition) to the monitor.
warning	Send warning events (severity level 4—system has warning conditions) to the monitor.
notification	Send notifications (severity level 5—normal but significant conditions) to the monitor.
information	Send informational messages (severity level 6) to the monitor.
debugging	Send debug level messages (severity level 7) to the monitor.

Default Not set (no logging)

Mode Global configuration

logging single-priority

Description Configure single-priority logging to log one specific severity level from among the standard syslog message severity levels.

Syntax

```
[no] logging single-priority {emergency | alert | critical |
error |
warning | notification | information | debugging}
```

Parameter	Description
emergency	Log emergency events (severity level 0—system unusable) only.
alert	Log alert events (severity level 1—take action immediately) only.
critical	Log critical events (severity level 2—system is in critical condition) only.
error	Log error events (severity level 3—system has an error condition) only.
warning	Log warning events (severity level 4—system has warning conditions) only.
notification	Log notifications (severity level 5—normal but significant conditions) only.
information	Log informational messages (severity level 6) only.
debugging	Log debug level messages (severity level 7) only.

Default Not set (no logging)

Mode Configuration mode

logging syslog

Description Set the syslog logging level for events sent to the syslog host.

Syntax

```
[no] logging syslog
{disable | emergency | alert | critical | error | warning |
 notification | information | debugging}
```

Parameter	Description
disable	Disable logging of syslog events.
emergency	Send emergency events (severity level 0—system unusable) to the syslog host.
alert	Send alert events (severity level 1—take action immediately) to the syslog host.
critical	Send critical events (severity level 2—system is in critical condition) to the syslog host.
error	Send error events (severity level 3—system has an error condition) to the syslog host.
warning	Send warning events (severity level 4—system has warning conditions) to the syslog host.
notification	Send notifications (severity level 5—normal but significant conditions) to the syslog host.
information	Send informational messages (severity level 6) to the syslog host.
debugging	Send debug level messages (severity level 7) to the syslog host.

Default Not set (no logging)

Mode Global configuration

logging trap

Description Set the logging level for traps sent to the SNMP host.

Syntax

```
[no] logging trap {disable | emergency | alert | critical}
```

Parameter	Description
disable	Disable logging of SNMP traps.
emergency	Sent emergency events (severity level 0—system unusable) to the SNMP host.
alert	Send alert events (severity level 1—take action immediately) to the SNMP host.

Parameter	Description
critical	Send critical events (severity level 2—system is in critical condition) to the SNMP host.

Default Not set (no logging)

Mode Global configuration

mac-address

Description Configure a static MAC address.

Syntax

```
[no] mac-address mac-address port port-num vlan vlan-id
[trap {dest}]
```

Parameter	Description
mac-address	Hardware address, in the following format: *aabb.ccdd.eeff*
port *port-num*	ACOS Ethernet port to which to assign the MAC address. If the ACOS device is a member of an aVCS virtual chassis, specify the interface as follows: *DeviceID*/*Portnum*
vlan *vlan-id*	Layer 2 broadcast domain in which to place the device.
trap	Send packets to the CPU for processing, instead of switching them in hardware: • **dest** – Send packets that have this MAC as a destination address to the CPU.

NOTE: The **trap** option is supported on only some FTA Thunder platform: Thunder 6655, Thunder 7650, Thunder 8665S, and Thunder 7460.

Default No static MAC addresses are configured by default.

Mode Configuration mode

Example The following command configures static MAC address abab.cdcd.efef on port 5 in VLAN 3:

```
ACOS(config)# mac-address abab.cdcd.efef port 5 vlan 3
```

mac-age-time

Description Set the aging time for dynamic (learned) MAC entries. An entry that remains unused for the duration of the aging time is removed from the MAC table.

Syntax

```
[no] mac-age-time seconds
```

Replace seconds with the number of seconds a learned MAC entry can remain unused before it is removed from the MAC table (10-600).

Default 300 seconds

Mode Configuration mode

On some Thunder models, the actual MAC aging time can be up to 2 times the configured value. For example, if the aging time is set to 50 seconds, the actual aging time will be between 50 and 100 seconds. (This applies to the AX 3200-12, AX 3400, AX 5200-11 and AX 5630.)

On other models, the actual MAC aging time can be +/- 10 seconds from the configured value.

Example The following command changes the MAC aging time to 600 seconds:

```
ACOS(config)# mac-age-time 600
```

maximum-paths

Description Change the maximum number of paths a route can have in the Forwarding Information Base (FIB).

Syntax

```
[no] maximum-paths num
```

Replace *num* for the maximum number of paths a route can have. You can specify 1-64.

Default 4

Mode Global configuration

Usage The maximum-paths command can also be used within the configuration level for specific routing protocols (for example, BGP and OSPF). When used in this manner, the number of maximum paths used in the routing protocol configuration overrides the number set at the global configuration level.

Example The following example sets the number of maximum paths to 8 at the global configuration level, and to 6 at the BGP configuration level:

```
ACOS(config)# maximum-paths 8
ACOS(config)# router bgp 102
ACOS(config-bgp:102)# maximum-paths 6
```

In this example, the final ECMP for BGP routes in the FIB is 6; for all other routing protocols, it can be 8.

merge-mode-add

Description Use this command to enter “merge” mode and integrate new configurations into the current running configuration. This is a setting of the “block-merge” command in which any child instances of the old configuration are retained if not present in the new configuration.

Syntax `merge-mode-add slb {server | service-group | virtual-server}`

Parameter	Description
server	Controls block-merge behavior for slb server.
service-group	Controls block-merge behavior for slb service-group.
virtual-server	Controls block-merge behavior for slb virtual-server.

Default N/A

Mode Block-merge configuration mode

mirror-port

Description Specify a port to receive copies of another port's traffic.

For more information, see "Multiple Port-Monitoring Mirror Ports" in the *System Configuration and Administration Guide*.

Syntax

```
[no] mirror-port portnum ethernet  portnum [input | output | both]
```

Parameter	Description
mirror-port *portnum*	Mirror port index number.
ethernet *portnum*	Ethernet port number. This is the port that will act as the mirror port. Mirrored traffic from the monitored port will be copied to and sent out of this port.
input	Configures the mirror port so that only inbound traffic from the monitored port can be sent out of the mirror port.
output	Configures the mirror port so that only outbound traffic from the monitored port can be sent out of the mirror port.
both	Configures the mirror port so that both inbound and outbound traffic from the monitored port can be sent out of the mirror port. This is the default behavior, meaning that if no traffic direction is specified, then both inbound and outbound traffic will be mirrored without having to explicitly specify the **both** option.

Default Not set

Mode Configuration mode

Usage When enabling monitoring on a port, you can specify the mirror port to use. You also can specify the traffic direction. A monitored port can use multiple mirror ports.

To specify the port to monitor, use the **monitor** command at the interface configuration level.

Example The following command configures Ethernet port 4 so that it is able to send both inbound and outbound traffic from the monitored port:

```
ACOS(config)# mirror-port 1 ethernet 4 both
```

The following commands configure a monitor port, Ethernet port 8, to use Ethernet port 4 as the mirror port, using mirror index 1 from above:

```
ACOS(config)# inferface ethernet 8
ACOS(config-if:ethernet:8)# monitor 1 both
```

Example The following command configures Ethernet port 3 to send only inbound traffic from the monitored port:

```
ACOS(config)# mirror-port 2 ethernet 3 input
```

The following commands configure a monitor port, Ethernet port 6, to use Ethernet port 3 as the mirror port, using mirror index 2 from above. Note that the **input** parameter must be used on the monitor port since the mirror port was also configured with the **input** parameter:

```
ACOS(config)# inferface ethernet 6
ACOS(config-if:ethernet:6)# monitor 2 input
```

Related Commands:

- monitor

monitor

Description Specify event thresholds for utilization of resources.

Syntax

```
[no] monitor resource-type threshold-value
```

Parameter	Description
resource-type	Type of resource for which to set the monitoring threshold: • **buffer-drop** – Packet drops (dropped IO buffers) • buffer-usage – Control buffer utilization

Parameter	Description
	The **conn-type** resources configure the conn resource type thresholds per CPU: • **conn-type0** – 32 bytes • **conn-type1** – 64 bytes • **conn-type2** – 128 bytes • **conn-type3** – 256 bytes • **conn-type4** – 512 bytes • **ctrl-cpu** – Control CPU utilization • **data-cpu** – Data CPUs utilization • **disk** – Hard disk utilization • **memory** – Memory utilization The **smp-type** resources configure the Threshold for SMP resources for the global session memory pool, shared across all of the ACOS device's CPUs: • **smp-type0** – 32 bytes • **smp-type1** – 64 bytes • **smp-type2** – 128 bytes • **smp-type3** – 256 bytes • **smp-type4** – 512 bytes • **warn-temp** – CPU temperature
threshold-value	The values you can specify depend on the event type and on the ACOS device model.

Default The default threshold values depend on the event type and on the ACOS model.

Usage If utilization of a system resource crosses the configured threshold, a log message is generated. If applicable, an SNMP trap is also generated.

The show monitor command is used to display the configured event thresholds.

Example The following command sets the event threshold for data CPU utilization to 80%:

```
ACOS(config)# monitor data-cpu 80
```

multi-config

Description Enable simultaneous admin sessions.

Syntax

```
[no] multi-config enable
```

Default Enabled

Mode Config

Usage Use the “no” form of the command to disable multiple admin access.

NOTE: Disabling multiple admin access does not terminate currently active admin sessions. For example, if there are 4 active config sessions, disabling multi-user access will cause the display of a permission prompt when a 5th user attempts to log onto the device. However, the previous 4 admin sessions will continue to run unaffected.

multi-ctrl-cpu

Description Assigns more than one CPU for control plane processing.

NOTE:

- Not all devices support this command.
- After multi-ctrl-cpu is configured, changing the number of vCPUs is not supported. To change the vCPUs, first unconfigure the multi-ctrl-cpus, and then change the vCPUs.

Syntax

```
multi-ctrl-cpu [num]
```

[num] is the required amount of control CPU.

Limitation The number of control CPUs has the following limitations:

- The number of control CPUs must be less than half of the total number of CPUs. This is calculated on a ratio basis.
- The maximum number of control CPUs is 8.
- The number of CPUs configured on vThunder must be 8 or more.

Default One CPU is used for control processing.

Mode Global configuration level

Usage This command enables the utilization of multiple CPUs for control plane processing. To view the number of CPUs statistics, use the show hardware command.

Consider the following points:

- The `multi-ctrl-cpu` command applies per disk partition only (Primary and Secondary). If rebooted from a different disk partition, the command must be applied again on the new partition.
- The **`no`** syntax is unavailable for this command. To disable multiple CPUs for control processing and restore it to default, configure **`multi-ctrl-cpu 1`**.

NOTE:

- A device reboot is required to activate the newly assigned value.
- It is highly recommended to set the global health monitoring to the same value as the number of control CPUs to avoid any imbalance.

Example Determine the number of CPUs available to and for the system using the **`show hardware`** command.

```
ACOS(config)# show hardware
Thunder Series Unified Application Service Gateway vThunder
Serial No vThunder05657C805BC02413712A736A476AFCFF368AF83E
CPU         : Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz
8 cores
2 stepping
Storage     : Single 30G drive, Free storage is 13G
Memory      : Total System Memory 8126 Mbytes, Free Memory 3877
Mbytes
```

```
L2/3 ASIC   : 0 device(s) present
Ports       : 4
Flags       : No CF
SMBIOS      : Build  6.00
12/12/2018
```

For control processing, there is always one control CPU for control processing, and there are two control CPUs by default for high-end hardware devices. To view this data, use **show cpu** command.

In the below example, the ratio setup is 1:7. 1 Control CPU : 5 Data + 2 I/O CPU's.

```
ACOS(config)# show cpu
Time: Apr-21-2022, 20:49
1Sec       5Sec     10Sec      30Sec      60Sec
------------------------------------------------------------
Control1          8%         9%         9%         9%         9%
Data1             0%         0%         0%         0%         0%
Data2             0%         0%         0%         0%         0%
Data3             0%         0%         0%         0%         0%
Data4             0%         0%         0%         0%         0%
Data5             0%         0%         0%         0%         0%
I/O1              0%         0%         0%         0%         0%
I/O2              0%         0%         0%         0%         0%
```

In the below example, the first attempt to set four control CPUs will fail since the system detects a 4:4 ratio and result in a backend error.

```
ACOS(config)# multi-ctrl-cpu 4
This will modify your boot profile for requested number of
control CPUs.
It will take effect after the next reboot.
Please confirm if you want to continue (Y/N)?: y
Backend Error: The number of control CPUs should be less than
half of the total number of CPUs.
```

The example setup has 8 CPUs available. Therefore, the supported ratio for the number of control CPUs to data CPUs is 1:7, 2:6 or 3:5. The next attempt to set three control CPUs will pass since the system detects a 3:5 ratio.

```
ACOS# multi-ctrl-cpu 3
```

```
This will modify your boot profile for requested number of
control CPUs.
It will take effect after the next reboot.
Please confirm if you want to continue (Y/N)?: y
Requested control-CPU configuration will run when the system
comes back up after the reboot.
Please reboot the system when you are ready.
```

NOTE: The 'reload' command does not reassign the CPUs function.

After rebooting the system, use the **show running-config** command to view the multiple CPUs assigned.

```
ACOS(config)# show running-config
!Current configuration: 219 bytes
!Configuration last updated at 08:42:18 IST Wed Apr 6 2022
!Configuration last saved at 08:42:18 IST Wed Apr 6 2022
!64-bit Advanced Core OS (ACOS) version 5.2.1-p4, build 95
(Feb-01-2022,05:15)
!
! multi-ctrl-cpu 3
!
--MORE—
```

Similarly, use the **show version** command to view the control CPU's assigned to the control processes.

```
ACOS# show version
Thunder Series Unified Application Service Gateway vThunder
Copyright 2007-2022 by A10 Networks, Inc.  All A10 Networks
products are
protected by one or more of the following US patents:
10749904, 10742559, 10735267, 10708150, 10686683,6970933,
6473802, 6374300
64-bit Advanced Core OS (ACOS) version 5.2.1-p4, build 95
(Feb-01-2022,05:15)
Booted from Hard Disk primary image
Number of control CPUs is set to 3
Serial Number:
vThunder05657C805BC02413712A736A476AFCFF368AF83E
aFleX version: 2.0.0
--MORE—
```

To view the status of all the available CPUs, use the **show cpu** command.

```
ACOS(config)# show cpu
Time: Apr-21-2022, 20:49
1Sec      5Sec     10Sec      30Sec      60Sec
------------------------------------------------------------
Control1          8%         9%         9%         9%         9%
Control2          4%         4%         4%         3%         3%
Control3          2%         2%         2%         3%         4%
Data1             0%         0%         0%         0%         0%
Data2             0%         0%         0%         0%         0%
Data3             0%         0%         0%         0%         0%
I/O1              0%         0%         0%         0%         0%
I/O2              0%         0%         0%         0%         0%
```

netflow common max-packet-queue-time

Description Specify the maximum amount of time ACOS can hold onto a NetFlow record packet in the queue before sending it to the NetFlow collector. ACOS holds a NetFlow packet in the queue until the packet payload is full of record data or until the queue timer expires.

Syntax

```
[no] netflow common max-packet-queue-time queue-time-multiplier
```

Replace *queue-time-multiplier* with the multiplier for the maximum queue time. Multiply this value by 20 to calculate the maximum number of milliseconds (ms) ACOS will hold a NetFlow packet in the queue before sending it. The multiplier can be 0-50. For example, to specify a half-second maximum queue time, set the multiplier to 25. Likewise, to specify a 1-second queue time, set the multiplier to 50.

Setting the multiplier to 0 means that there will be no delay for NetFlow packets to be sent to the NetFlow collector, and NetFlow records will not be buffered.

Default 50 (1-second maximum queue time)

Mode Global configuration level

netflow monitor

Description Enable ACOS to act as a NetFlow exporter, for monitoring traffic and exporting the data to one or more NetFlow collectors for analysis.

Syntax

```
[no] netflow monitor  monitor-name
```

Default Replace *monitor-name* with the name of the NetFlow monitor.

This command changes the CLI to the configuration level for the specified NetFlow monitor, where the following commands are available.

Command	Description
[no] custom-record *options*	Configure the custom record events to be exported: • sesn-event-nat44-creation – Export NAT44 session creation events • sesn-event-nat44-deletion – Export NAT44 session deletion events • sesn-event-nat64-creation – Export NAT64 session creation events • sesn-event-nat64-deletion – Export NAT64 session deletion events • sesn-event-dslite-creation – Export Dslite session creation events • sesn-event-dslite-deletion – Export Dslite session deletion events • sesn-event-fw4-creation – Export FW4 session creation events • sesn-event-fw4-deletion – Export FW4 session deletion events • sesn-event-fw6-creation – Export FW6 session creation events • sesn-event-fw6-deletion – Export FW6 session deletion events

Command	Description
	• deny-reset-event-fw4 – Export FW4 Deny Reset events • deny-reset-event-fw6 – Export FW6 Deny Reset events • port-mapping-nat44-creation – Export NAT44 Port Mapping Creation Event • port-mapping-nat44-deletion – Export NAT44 Port Mapping Deletion Event • port-mapping-nat64-creation – Export NAT64 Port Mapping Creation Event • port-mapping-nat64-deletion – Export NAT64 Port Mapping Deletion Event • port-mapping-dslite-creation – Export Dslite Port Mapping Creation Event • port-mapping-dslite-deletion – Export Dslite Port Mapping Deletion Event • port-batch-nat44-creation – Export NAT44 Port Batch Creation Event • port-batch-nat44-deletion – Export NAT44 Port Batch Deletion Event • port-batch-nat64-creation – Export NAT64 Port Batch Creation Event
[**no**] **custom-record** *options (cont.)*	• port-batch-nat64-deletion – Export NAT64 Port Batch Deletion Event • port-batch-dslite-creation – Export Dslite Port Batch Creation Event • port-batch-dslite-deletion – Export Dslite Port Batch Deletion Event • port-batch-v2-nat44-creation – Export NAT44 Port Batch v2 Creation Event

Command	Description
	• port-batch-v2-nat44-deletion – Export NAT44 Port Batch v2 Deletion Event • port-batch-v2-nat64-creation – Export NAT64 Port Batch v2 Creation Event • port-batch-v2-nat64-deletion – Export NAT64 Port Batch v2 Deletion Event • port-batch-v2-dslite-creation – Export Dslite Port Batch v2 Creation Event • port-batch-v2-dslite-deletion – Export Dslite Port Batch v2 Deletion Event
[**no**] **destination** *ipaddr* [*portnum*]	Configure the destination where NetFlow records will be sent.
disable	Disable this NetFlow monitor.
[**no**] **flow-timeout**	Timeout value interval at which flow records will be periodically exported for long-lived sessions. Flow records for short-lived sessions (if any) are sent upon termination of the session. After the specified amount of time has elapsed, the ACOS device will send any flow records to the NetFlow collector, even if the flow is still active. The flow timeout can be set to 0-1440 minutes. The flow timeout default value is 10 minutes. **NOTE:** Apart from flow records (in case of fixed templates) this statement holds true for session deletion records (in case of custom records) as well. Setting the timeout value to 0 disables the flow timeout feature. Regardless of how long-lived a

Command	Description
	flow might be, the ACOS device waits until the flow has ended and the session is deleted before it sends any flow records for it.
`[no] protocol`	Configure the version of the NetFlow protocol you want to use: • **v9** – Version 9 (default) • **v10** – Version 10 (IPFIX)
`[no] record` *netflow-template-type*	Configure the NetFlow record types to be exported. • `dslite` – Export DS-Lite Flow Record Template • `nat44` – Export NAT44 Flow Record Template • `nat64` – Export NAT64 Flow Record Template • `netflow-v5` – Export NetFlow V5 Flow Record Template • `netflow-v5-ext` – Export extended NetFlow V5 Flow Record Template, supports ipv6 • `port-batch-dslite` – Export DS-Lite Port Batching Event Template • `port-batch-nat44` – Export NAT44 Port Batching Event Template • `port-batch-nat64` – Export NAT64 Port Batching Event Template • `port-batch-v2-dslite` – Export DS-Lite NAT Port Batching v2 Event Template • `port-batch-v2-nat44` – Export NAT44 NAT Port Batching v2 Event Template • `port-batch-v2-nat64` – Export NAT64 NAT Port Batching v2 Event Template • `port-mapping-dslite` – Export DS-Lite Port Mapping Event Template

Command	Description
	• `port-mapping-nat44` – Export NAT44 Port Mapping Event Template • `port-mapping-nat64` – Export NAT64 Port Mapping Event Template • `sesn-event-dslite` – Export DS-Lite Session Event Template • `sesn-event-fw4` – Export FW Ipv4 Session Event Template • `sesn-event-fw6` – Export FW Ipv6 Session Event Template • `sesn-event-nat44` – Export NAT44 Session Event Template • `sesn-event-nat64` – Export NAT64 Flow Record Template For more information, see "NetFlow v9 and v10 (IPFIX)" chapter in the *System Configuration and Administration Guide*.
`[no]` **`resend-template`** `{`**`records`***`num`* `|` **`timeout`** *`seconds`*`}`	Configure when to resend the NetFlow template. The trigger can be either the number of records, or the amount of time that has passed. • **`records`** – Specifies the counters by which the ACOS device resends templates to the collectors. The *num* can be 0-1000000. The default is 1000. • **`timeout`** – Specifies the time between when templates are resent to the collectors. The *`num`* is the number of seconds and can be 0-86400. The default is 1800. **NOTE:** Specifying 0 means never resend the template.
`[no]` **`sample`**	Enable sampling.

Command	Description
{**ethernet** | **global** | **nat-pool** | **ve**}	Configure filters for monitoring traffic. Identify the specific type and subset of resources to monitor. • **ethernet** *portnum* – Specify the list of Ethernet data ports to monitor. Flow information for the monitored interfaces is sent to the NetFlow collector(s). • **global** – (Default) No filters are in effect. Traffic on all interfaces is monitored. • **nat-pool** *pool-name* – NAT pool. • **ve** *ve-num* – Specify the list of Virtual Ethernet (VE) data ports to monitor.
[**no**] **source-address** {**ip** *ipv4addr* | **ipv6** *ipv6addr*}	Uses the specified IP address as the source address for exported NetFlow packets. By default, the IP address assigned to the egress interface is used. This command does not change the egress port out which the NetFlow traffic is exported.
[**no**] **source-ip-use-mgmt**	Use the management interface's IP address as the source IP for exported NetFlow packets. This command does not change the egress port out which the NetFlow traffic is exported.
[no] user-tag *user-tag-name*	Custom tag that can then be searched by using the aXAPI.
[no] disable-log-by-destination	Command in netflow monitor configuration mode are available for disabling of logging by destination protocol and port. Following are the sub-commands under this mode.
[no] icmp	Disable logging for ICMP traffic.
[no] others	Disable logging for L4 protocol traffic that is not

Command	Description
	TCP or UDP.
`[no] tcp`	Disable logging for TCP traffic.
`[no] udp`	Disable logging for UDP traffic.

Default Described above, where applicable.

Mode Global configuration level

Related Commands:

- Tagging Objects

netflow template

Description Creates a custom NetFlow (IPFIX) template by configuring the exact Information Elements (IEs) to be logged.

Syntax

```
[no] netflow template  template-name
```

Default Replace *template-name* with the name of the NetFlow template.

This command changes the CLI to the configuration level for the specified NetFlow template, where the following commands are available.

Command	Description
`[no] information-element` *options*	Command in NetFlow template configuration mode that places you in a sub-configuration mode, where the commands in Table 12 are available for configuring one or more information elements.
`[no] template-id` *num*	Configure the custom IPFIX Template ID. The *num* can be 2001-3000. • The template IDs must be unique across different templates. ACOS displays an error message if two templates with the same template ID are bound to any NetFlow monitor.

Command	Description
	• The template IDs should not be reused until after a time period exceeding 3 times the retransmission delay. ACOS displays an error message when a template with such template ID is bound to a NetFlow monitor. [RFC: Template IDs may be re-used by Exporting Processes by exporting a new Template for the Template ID after waiting at least 3 times the retransmission delay.]

Table 12 : Sub-Commands in the netflow template information-element Configuration Mode

Command	Description
`fwd-tuple-vnp-id`	Session forward tuple partition id (ID: 33028)
`rev-tuple-vnp-id`	Session reverse tuple partition id (ID: 33029)
`source-ipv4-address`	IPv4 source address in the IP packet header (ID: 8)
`source-ipv4-prefix-len`	Prefix length for IPv4 source address (ID: 9)
`dest-ipv4-address`	IPv4 destination address in the IP packet header (ID: 12)
`dest-ipv4-prefix-len`	Prefix length for IPv4 dest address (ID: 13)
`source-ipv6-address`	IPv6 source address in the IP packet header (ID: 27)
`source-ipv6-prefix-len`	Prefix length for IPv6 source address (ID: 29)
`dest-ipv6-address`	IPv6 destination address in the IP packet header (ID:28)

Table 12 : Sub-Commands in the netflow template information-element Configuration Mode

Command	Description
dest-ipv6-prefix-len	Prefix length for IPv6 dest address (ID: 30)
post-nat-source-ipv4-address	IPv4 natted source address (ID: 225)
post-nat-dest-ipv4-address	IPv4 natted destination address (ID: 226)
post-nat-source-ipv6-address	IPv6 natted source address (ID: 281)
post-nat-dest-ipv6-address	IPv6 natted destination address (ID: 282)
source-port	Source port identifier in the transport header (ID: 7)
dest-port	Destination port identifier in the transport header (ID: 11)
post-nat-source-port	L4 natted source port (ID: 227)
post-nat-dest-port	L4 natted destination port (ID: 228)
fwd-tuple-type	Session forward tuple type (ID: 33024)
rev-tuple-type	Session reverse tuple type (ID: 33025)
ip-proto	Value of the protocol number in the IP packet header (ID: 4)
flow-direction	Flow direction: 0:inbound(To an outside interface)/1:outbound(To an inside interface) (ID: 61)
tcp-control-bits	Cumulative of all the TCP flags seen for this flow (ID: 6)

Table 12 : Sub-Commands in the netflow template information-element Configuration Mode

Command	Description
fwd-bytes	Incoming bytes associated with an IP Flow (ID: 1)
fwd-packets	Incoming packets associated with an IP Flow (ID: 2)
rev-bytes	Delta bytes in reverse direction of bidirectional flow record (ID: 32769)
rev-packets	Delta packets in reverse direction of bidirectional flow record (ID: 32770)
in-port	Incoming interface port (ID: 10)
out-port	Outgoing interface port (ID: 14)
in-interface	Incoming interface name e.g. ethernet 0 (ID: 82)
out-interface	Outgoing interface name e.g. ethernet 0 (ID: 32850)
port-range-start	Port number identifying the start of a range of ports (ID: 361)
port-range-end	Port number identifying the end of a range of ports (ID: 362)
port-range-step-size	Step size in a port range (ID: 363)
port-range-num-ports	Number of ports in a port range (ID: 364)
rule-name	Rule Name (ID: 33034)
rule-set-name	Rule-Set Name (ID: 33035)
fw-source-zone	Firewall Source Zone Name (ID: 33036)
fw-dest-zone	Firewall Dest Zone Name (ID: 33037)
application-id	Application ID (ID: 95)
application-name	Application ID (ID: 96)
application-category-name	Application first level category name (ID: 372)
application-	Application second level category name (ID: 373)

Table 12 : Sub-Commands in the netflow template information-element Configuration Mode

Command	Description
subcategory-name	
radius-imsi	Radius Attribute IMSI (ID: 455)
radius-msisdn	Radius Attribute MSISDN (ID: 456)
radius-imei	Radius Attribute IMEI (ID: 33030)
radius-custom1	Radius Attribute Custom 1 (ID: 33031)
radius-custom2	Radius Attribute Custom 2(ID: 33032)
radius-custom3	Radius Attribute Custom 3 (ID:33033)
flow-start-msec	The absolute timestamp of the first packet of the flow (ID: 152)
flow-end-msec	The absolute timestamp of the last packet of the flow (ID: 153)
flow-duration-msec	Difference in time between the first observed packet of this flow and the last observed packet of this flow (4 bytes) (ID: 161)
flow-duration-msec-64	Difference in time between the first observed packet of this flow and the last observed packet of this flow (8 bytes) (ID: 33039)
nat-event	Indicates a NAT event (ID: 230)
fw-event	Indicates a FW session event (ID: 233)
fw-deny-reset-event	Indicates a FW deny/reset event (ID: 33038)
cgn-flow-direction	Flow direction: 0:inbound(To an outside interface)/1:outbound(To an inside interface)/2:hairpin(From an inside interface to an inside interface) (ID: 33040)

netflow use-partition

Description Configure a dedicated partition to send the NetFlow logs.

NOTE: You cannot configure the **netflow monitor** command when this command is configured.

Syntax

```
[no] netflow use-partition  partition-name
```

Replace *partition-name* with the name of the dedicated partition.

Command	Parameter
[no] use-partition *partition-name*	Specify the dedicated partition name to send the NetFlow logs. **NOTE:** You cannot configure **netflow use-partition** if NetFlow is already configured (and vice versa).

Mode Configuration mode

Example In the following example, the partition P1 is used for NetFlow logging:

```
ACOS(config)# netflow use-partition P1
```

no

Description Remove a configuration command from the running configuration or negate a command or set it to its default setting.

Syntax

```
no command-string
```

Default N/A

Mode All

Usage Use the “no” form of a command to disable a setting or remove a configured item. Configuration commands at all Config levels of the CLI have a “no” form, unless otherwise noted.

The command is removed from the running-config. To permanently remove the command from the configuration, use the write memory command to save the configuration changes to the startup-config.

Example The following command removes server “http99” from the running-config:

```
ACOS(config)# no slb server http99
```

Example The following command disables the terminal command history feature:

```
ACOS(config)# no terminal history
ACOS#
```

ntp

Description Configure Network Time Protocol (NTP) parameters.

Syntax

```
[no] ntp auth-key {M | SHA | SHA1} [hex] string
```

Syntax

```
[no] ntp trusted-key ID-num
```

Syntax

```
[no] ntp server {hostname | ipaddr}
```

The **ntp server** command changes the CLI to the configuration level for the server, where the following commands are available.

Parameter	Description
disable	Disables synchronization with the NTP server.
enable	Enables synchronization with the NTP server.
key *ID-num*	Creates an authentication key. For *ID-num*, enter a value between 1-65535.
prefer	Directs ACOS to use this NTP server by default. Additional NTP servers are used as backup servers if the preferred NTP server is unavailable.
{**M** | **SHA** | **SHA1**} {**ascii** | **hex**} *string*	Specifies the type of authentication key you want to create for authenticating the NTP servers. • **M** - encryption using MD5 • **SHA** - encryption using SHA • **SHA1** - encryption using SHA1 Specify the authentication key *string* (1-20

Parameter	Description
	characters. Use the **hex** parameter to specify the *string* in hex format (21-40 characters), or **ascii** to specify it in text.
trusted-key *ID-num*	Adds an authentication key to the list of trusted keys. For *num*, enter the identification number of a configured authentication key to add the key to the trusted key list. You can enter more than one number, separated by whitespace, to simultaneously add multiple authentication keys to the trusted key list.

Default NTP synchronization is disabled by default. If you enable it, DST is enabled by default, if applicable to the specified timezone.

Mode Configuration mode

Usage You can configure a maximum of 4 NTP servers.

If the system clock is adjusted while OSPF or IS-IS is enabled, the routing protocols may stop working properly. To work around this issue, disable OSPF and IS-IS before adjusting the system clock.

Example The following commands configure an NTP server and enable NTP:

```
ACOS(config)# ntp server 10.1.4.20
ACOS(config)# ntp server enable
```

Example The following example creates 3 authentication keys (1337 using MD5 encryption, 1001 using SHA encryption, and 1012 using SHA1 encryption) and adds these keys to the list of trusted keys. The NTP server located at 10.1.4.20 is configured to use a trusted key (1337) for authentication:

```
ACOS(config)# ntp auth-key 1337 M XxEnc192
ACOS(config)# ntp auth-key 1001 SHA Vke1324as
ACOS(config)# ntp auth-key 1012 SHA1 28fj039
ACOS(config)# ntp trusted-key 1337 1001 1012
ACOS(config)# ntp server 10.1.4.20 key 1337
```

You can verify the NTP server and authentication key configuration with the **show run** command. The following example includes an output modifier to display only NTP-related configuration:

```
ACOS(config)# show run | include ntp
ntp auth-key 1001 SHA encrypted
FSNiuf10Dtzc4aY0tk2J4DwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2w
Dn
ntp auth-key 1012 SHA1 encrypted
NEMuh8GgapM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2w
Dn
ntp auth-key 1337 M encrypted
zIJptJHuaQaw/5o10esBTDwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2w
Dn
ntp trusted-key 1001 1012 1337
ntp server 10.1.4.20 key 1337
ntp server enable
```

object-group network

Description Create a network object group, for specifying match criteria using Layer 3 parameters. An object group is a named set of IP addresses or protocol values.

Syntax

```
[no] object-group network group-name [acl | fw {v4 | v6}]
```

Parameter	Description
group-name	Name of the network object group (1-63 characters).
acl	Create a network object group that will be used by Access Control Lists. When you configure an IPv4 or IPv6 ACL, you can specify the name of an object group in place of IP address or protocol parameters. This capability can be useful in cases where the same match criteria are used in more than one ACL. If you need to modify the match criteria, you can apply the changes to all affected ACLs at the same time, by modifying the object group. You

Parameter	Description
	do not need to edit each individual ACL.
fw v4	Create a network object group that will be used for IPv4 firewall configurations.
f4 v6	Create a network object group that will be used for IPv4 firewall configurations.

This command changes the CLI to the configuration level for the network object group, where the following commands are available:

Command	Description
[**no**] **any**	Matches on all IP addresses.
[**no**] **description** *string*	Description (1-128 characters) of the object group instance being configured. The description string can be any combination of letters and numbers and is common for all objects in the group. You can specify the *group-name* of the object group in the description.
[**no**] **host***host-src-ipaddr*	Matches only on the specified host IPv4 or IPv6 address.
[**no**] *net-src-ipaddr* { *filter-mask* | **/***mask-length* }	Matches on any host in the specified IPv4 subnet. The *filter-mask* specifies the portion of the address to filter: • Use 0 to match. • Use 255 to ignore. For example, the following *filter-mask* filters on a 24-bit subnet: 0.0.0.255 Alternatively, you can use *mask-length* to specify the portion of the address to filter. For example, you can specify “/24” instead “0.0.0.255” to filter on a 24-bit subnet.

Command	Description
[**no**] *net-src-ipv6addr* **/***prefix-length*	Matches on any host in the specified subnet. The *prefix-length* specifies the portion of the address to filter.
[**no**] *sequence-number*	Specify a sequence number (1-8192). Sequence numbers can be used to maintain the order of the members in the object group.

Default Not set

Mode Configuration mode

Example The following commands configure network object groups INT_CLIENTS, HTTP_SERVERS and FTP_SERVERS:

```
ACOS(config)# object-group network INT_CLIENTS
ACOS(config-network-group:INT_CLIENTS)# host 10.9.9.1
ACOS(config-network-group:INT_CLIENTS)# host 10.9.9.2
ACOS(config-network-group:INT_CLIENTS)# 10.1.0.0 0.0.255.255
ACOS(config-network-group:INT_CLIENTS)# 10.2.0.0 0.0.255.255
ACOS(config-network-group:INT_CLIENTS)# exit
ACOS(config)# object-group network HTTPS_SERVERS
ACOS(config-network-group:HTTPS_SERVERS)# host 192.168.230.215
ACOS(config-network-group:HTTPS_SERVERS)# host 192.168.230.216
ACOS(config-network-group:HTTPS_SERVERS)# host 192.168.230.217
ACOS(config-network-group:HTTPS_SERVERS)# exit
ACOS(config)# object-group network FTP_SERVERS
ACOS(config-network-group:FTP_SERVERS)# host 192.168.230.5
ACOS(config-network-group:FTP_SERVERS)# host 192.168.230.216
ACOS(config-network-group:FTP_SERVERS)# exit
```

Example Below is an example of how to enter a description for an object group.

```
ACOS(config)# object-group network s616844shsq101
ACOS(config-network-group:s616844shsq101)# description IP
address space for s616844shsq101 resource group
```

object-group service

Description Create a service object group, for specifying match criteria using Layer 4 - Layer 7 parameters. An object group is a named set of IP addresses or protocol values.

Usage `[no] object-group service group-name`

This command changes the CLI to the configuration level for the service object group, where the following commands are available:

Command	Description
`[no] description string`	Description (1-128 characters) of the object group instance being configured. The description string can be any combination of letters and numbers and is common for all objects in the group. You can specify the *group-name* of the object group in the description.
`[no] icmp [type {type-option} [code {any-code | code-num}]]`	Matches on ICMP traffic. The **type** *type-option* parameter matches based on the specified ICMP type. You can specify one of the following ICMP types (enter either the number or the name): • **any-type** – Matches on any ICMP type. • **dest-unreachable** | **3** – Type 3, destination unreachable • **echo-reply** | **0** – Type 0, echo reply • **echo-request** | **8** – Type 8, echo request • **info-reply** | **16** – Type 16, information reply • **info-request** | **15** – Type 15, information request • **mask-reply** | **18** – Type 18, address mask reply • **mask-request** | **17** – Type 17, address mask request

Command	Description
	• **parameter-problem** | **12** – Type 12, parameter problem • **redirect** | **5** – Type 5, redirect message • **source-quench** | **4** – Type 4, source quench • **time-exceeded** | **11** – Type 11, time exceeded • **timestamp** | **13** – Type 13, timestamp • **timestamp-reply** | **14** – Type 14, timestamp reply The **code** *code-num* option is applicable if the protocol type is **icmp**. You can specify: • **any-code** – Matches on any ICMP code. • *code-num* – ICMP code number, 0-254
[**no**] **icmpv6** [**type** {*type-option*} [**code** {**any-code** | *code-num*}]]	Matches on ICMPv6 traffic. The **type** *type-option* parameter matches based on the specified ICMPv6 type. You can specify one of the following types (enter either the number or the name): **any-type** – Matches on any ICMPv6 type. • **dest-unreachable** – Matches on type 1, destination unreachable messages. • **echo-reply** – Matches on type 129, echo reply messages. • **echo-request** – Matches on type 128, echo request messages. • **packet-too-big** – Matches on type 2, packet too big messages. • **param-prob** – Matches on type 4, parameter problem messages.

Command	Description
	• **time-exceeded** – Matches on type 3, time exceeded messages.
[**no**] **protocol-id***id*	Specify the protocol ID on which to match. For more information, see https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers for a list of protocol IDs and corresponding protocols.
{**tcp** | **udp**} **eq** *src-port* | **gt** *src-port* | **lt** *src-port* | **range** *start-src-port end-src-port*	Specifies the protocol ports on which to match: • **eq** *src-port* – The ACL matches on traffic on the specified port. • **gt** *src-port* – The ACL matches on traffic on any port with a higher number than the specified port. • **lt** *src-port* – The ACL matches on traffic on any port with a lower number than the specified port. • **range** *start-src-port end-src-port* – The ACL matches on traffic on any port within the specified range.

Default Not set

Mode Configuration mode

Example The following commands configure service object group WEB_SERVICES and display the configuration:

```
ACOS(config)# object-group service WEB-SERVICES
ACOS(config-service-group:WEB-SERVICES)# tcp eq 80
ACOS(config-service-group:WEB-SERVICES)# tcp source range 1025
65535 eq 8080
ACOS(config-service-group:WEB-SERVICES)# tcp source range 1025
65535 eq 443
ACOS(config-service-group:WEB-SERVICES)# exit
ACOS(config)# show object-group
object-group service WEB-SERVICES
tcp eq 80
```

```
tcp source range 1025 65535 eq 8080
tcp source range 1025 65535 eq 443
```

Example The following command configures an ACL that uses service object group configured above:

```
ACOS(config)# access-list 111 permit object-group WEB-SERVICES
any any
```

offload-cpus

Description This command implements generic CPU offloading infrastructure.

Set the number of offload CPUs. The maximum limit is platform dependent.

Syntax

```
[no]offload-cpus{1-12}
```

NOTE: This is a system-wide command; hence you must reboot the system after configuring the option to take effect.

Default Not set

Mode Configuration mode

Example The following commands configures the offload CPU feature:

```
ACOS(config)# offload-cpus 3
```

packet-handling

Description Configure how you want the system to handle unregistered broadcast packets.

Syntax

```
[no] packet-handling broadcast {trap | flood}
```

Parameter	Description
trap	Trap packets to the CPU.
flood	Flood packets to other ports.

Mode Configuration mode

ping

Description Ping is used to diagnose basic network connectivity. For syntax information, see ping.

poap

Description Enables Power On Auto Provisioning (POAP).

NOTE: After using the **poap** command, you must reboot the system. The device will return to service in POAP mode.

Syntax

```
[no] poap {enable | disable}
```

Default By default, the POAP mode is disabled on all physical devices.

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

NOTE: POAP mode is not available on the virtual platform.

radius-server

Description Set RADIUS parameters, for authenticating administrative access to the ACOS device.

Syntax

```
[no] radius-server host {hostname | ipaddr} secret  secret-string
  [acct-port  protocol-port]
  [auth-port  protocol-port]
  [retransmit  num]
  [timeout  seconds]
```

Default `[no] radius-server {default-privilege-read-write | message-authenticator-verify-enable}`

Parameter	Description
hostname | *ipaddr*	Hostname or IP address of the RADIUS server.

Parameter	Description
	secret *secret-string*[options]: Password, 1-128 characters, required by the RADIUS server for authentication requests. The following protocol options are used to manage RADIUS communication: • **acct-port***protocol-port*: Protocol port to which the ACOS device sends RADIUS accounting information. The default port is 1813. • **auth-port***protocol-port*: Protocol port to which the ACOS device sends authentication requests. The default port is 1812. • **retransmit** *num*: Maximum number of times the ACOS device can resend an unanswered authentication request to the server. If the ACOS device does not receive a reply to the final request, the ACOS device tries the secondary server, if one is configured. If no secondary server is available, or if the secondary server also fails to reply after the maximum number of retries, authentication fails and the

Parameter	Description
	admin is denied access. You can specify 0-5 retries. The default is 3 retries. • **timeout***seconds*: Maximum number of seconds the ACOS device will wait for a reply to an authentication request before resending the request. You can specify 1-15 seconds. The default is 3 seconds.
default-privilege-read-write	Change the default privilege authorized by RADIUS from read-only to read-write. The default privilege is used if the Service-Type attribute is not used, or the A10 vendor attribute is not used. This is disabled by default; if the Service-Type attribute is not used, or the A10 vendor attribute is not used, successfully authenticated admins are authorized for read-only access.
message-authenticator-verify-enable	Enables the verification of the Message-Authenticator attribute in RADIUS messages. This is disabled by default; if the Message-Authenticator attribute is missing, the response will be rejected. If the attribute is present, it will always be verified. When this is disabled, responses

Parameter	Description
	without the attribute will still be accepted for compatibility. **NOTE:** It is recommended to enable this field and configure the RADIUS server to support the Message-Authenticator attribute for enhanced security.

Default No RADIUS servers are configured by default. When you add a RADIUS server, it has the default settings described in the table above.

You can configure up to 2 RADIUS servers. The servers are used in the order in which you add them to the configuration. Thus, the first server you add is the primary server. The second server you add is the secondary (backup) server. Enter a separate command for each of the servers. The secondary server is used only if the primary server does not respond.

Mode Configuration mode

Example The following commands configure a pair of RADIUS servers and configure the ACOS device to use them first, before using the local database. Since 10.10.10.12 is added first, this server will be used as the primary server. Server 10.10.10.13 will be used only if the primary server is unavailable.

```
ACOS(config)# radius-server host 10.10.10.12 secret radp1
ACOS(config)# radius-server host 10.10.10.13 secret radp2
ACOS(config)# authentication type radius local
ACOS(config)# radius-server message-authenticator-verify-
enable
```

raid

Description Enter the configuration level for RAID, if applicable to your device model.

Syntax

```
raid
```

NOTE: RAID configuration should be performed only by or with the assistance of technical support. It is strongly advised that you do not experiment with these commands.

rba

rba enable

Description Enable Role-Based Access Control (RBA) configuration.

This feature supports the creation of multiple users, groups, and roles with varying degrees of permissions. RBA can limit the read/write privileges on different partitions and for different objects.

For more information, see “Role-Based Access Control” in the *Management Access and Security Guide*.

Syntax

```
rba enable
```

Mode Configuration mode.

rba disable

Description Disable Role-Based Access Control (RBA) configuration.

For more information, see “Role-Based Access Control” in the *Management Access and Security Guide*.

Syntax

```
rba disable
```

Mode Configuration mode.

rba group

Description Configure an RBA group.

For more information, see “Role-Based Access Control” in the *Management Access and Security Guide*.

Syntax

```
[no] rba group
  users
  partition
    roles | privileges
```

Mode Configuration mode

Example The following example defines an RBA group “slb-group.” The group has two users, “slb-user1” and “slb-user2.” Both users are granted write privileges on SLB server objects but read only privileges on all other SLB objects in partition “companyA”:

```
!
rba group slb-group
  user slb-user1
  user slb-user2
  partition companyA
    slb read
    slb.server write
```

rba role

Description Configure an RBA role.

For more information, see “Role-Based Access Control” in the *Management Access and Security Guide*.

Syntax

```
[no] rba role-name
  privileges
```

Mode Configuration mode.

Example The following example defines an RBA role “role1.” Any user assigned this role will have write access on SLB server objects, but read privileges on all other SLB objects.

```
!
rba role role1
  slb read
  slb.server write
```

rba user

Description Configure RBA for a user.

The user must be an existing admin account and can be authentication either locally or externally using LDAP, RADIUS, or TACACS+.

For more information, see “Role-Based Access Control” in the *Management Access and Security Guide*.

Syntax

```
[no] rba user username
  partition partition-name
    roles | privileges
```

Mode Configuration mode.

Example The following example configures RBA for user “user1”. In partition companyA, this user has read privileges for SLB virtual server objects, write privileges for SLB server objects, but no access to all other SLB objects. In partition companyB, this user has all privileges defined by RBA role “role1”:

```
!
rba user user1
  partition companyA
    slb no-access
    slb.server write
    slb.virtual-server read
  partition companyB
    role role1
!
```

resource-track

Description Create a failover template for tracking events such as the operational state of BGPs, gateways, interfaces, trunks, and VLANs and enabling policy-based failover to occur. Using a policy-based failover template, you can allocate a weight of 1-255 per event. When the event occurs, the cost of the template increases, possibly causing the failover.

For more information, see “Configuring Policy-Based Failover” in the *Scaleout Configuration Guide*.

Syntax

```
resource-track [resource track template name]
```

Replace `resource track template name` with the name that you are assigning for the failover policy template. This template must be associated to a particular Scaleout node to take effect.

The command changes to `config-resource-track` configuration level for the failover template, where the following commands are displayed:

Parameter	Description
[no] bgp	Specify the BGP IP address that needs to be tracked. If the BGP neighbor is unreachable, the cost of this event increases causing the failover.
[no] gateway	Specify the IP Address of an IPv4 or IPv6 default gateway that needs to be tracked. If a gateway stops responding, the cost of the event increases. The weight can be specified individually for each gateway's IP address that you configure in the tracking events list.
[no] ethernet	Specify a weight for each Ethernet interface that you are planning to track. If the link goes down on an Ethernet data port, the cost of the event increases. The weight can be specified individually for each Ethernet data port.
[no] route	If an IPv4 or IPv6 route matching the specified options is not in the data route table, the cost of the event increases.
[no] trunk	If the trunk or individual ports in the trunk go down, the cost of the event increases.
[no] VLAN	If ACOS stops detecting traffic on a VLAN, the cost of the event increases.

Default N/A

Mode Configuration mode

Usage Use this command on any ACOS device to track the events and execute failover actions via a policy-based failover template.

Example The following example creates a failover policy-based template named `template_1` and configures the events:

```
ACOS(config)#resource-track template_1
ACOS(config-resource-track:template_1)#bgp 12.12.10.1 weight
100
ACOS(config-resource-track:template_1)#gateway 10.10.10.1
weight 100
ACOS(config-resource-track:template_1)#gateway 10.10.10.1
weight 100
ACOS(config-resource-track:template_1)#interface ethernet 1
weight 40
ACOS(config-resource-track:template_1)#route 20.20.20.1 /24
weight 100
ACOS(config-resource-track:template_1)#trunk 1 weight 20
```

restore

Description Restore the startup-config, aFleX policy files, and SSL certificates and keys from a file previously created by the backup system command. The restored configuration takes effect following a reboot.

For more information, see "Restoring From a Backup" in the *System Configuration and Administration Guide*.

Syntax

```
restore [use-mgmt-port] url
```

Parameter	Description
use-mgmt-port	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the ACOS device attempts to use the data route table to reach the remote device through a data interface.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of

Parameter	Description
	the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long and supports the following special characters: `!#$()*+,-.;=^_`{|}~`  The following special characters are not supported:  `(blank space) "%&'/:<>?@[\]` To enter the entire URL: • **tftp://***host***/***file* • **ftp://**[*user@*]*host*[**:port**]*/file* • **scp://**[*user@*]*host/file* • **sftp://**[*user@*]*host/file*

Default N/A

Mode Configuration mode

Usage Do not save the configuration (**write memory**) after restoring the startup-config. If you do, the startup-config will be replaced by the running-config and you will need to restore the startup-config again.

To place the restored configuration into effect, reboot the ACOS device.

route-map

Description Configures a rule in a route map. You can use route maps to provide input to routing commands, like the “redistribute” or “default-information originate” command for BGP.

Syntax

```
[no] route-map map-name {deny | permit} sequence-num
```

Parameter	Description
map-name	Route map name.
deny | **permit**	Action to perform on data that matches the rule.
sequence-num	Sequence number of the rule within the route map, 1-65535. Rules are used in ascending sequence order. The action in the first matching rule is used, and no further matching is performed. You do not need to configure route map rules in numerical order. The CLI automatically places them in the configuration (running-config) in ascending numerical order.

This command changes the CLI to the configuration level for the specified route map rule, where the following commands are available.

Command	Description
match *attribute*	Specifies the match criteria for routes: • **match as-path** *list-id* – Matches on the BGP AS paths in the specified AS path list. • **match community** *list-id1* [*list-id2 ... list-idn*] – Matches on the BGP communities in the specified community list. When the command specifies multiple lists, the route must match on each list. • **match extcommunity** *list-id1* [*list-id2 ... list-idn*] – Matches on the BGP extended communities listed in the specified extended community list. When the command specifies multiple lists, the route must match on each list. • **match group** *num* {**active** | **standby**} – Matches on VRRP-A set ID and state (active or standby). • **match interface** {**ethernet** *portnum* | **loopback**

Command	Description
	num | **trunk** *num* | **ve** *ve-num*} – Matches on the data interface used as the first hop for a route. • **match ip address** {*acl-id* | **prefix-list** *list-name*} – Matches on the route IP addresses in the specified ACL or prefix list. • **match ip next-hop** {*acl-id* | **prefix-list** *list-name*}– Matches on the next-hop router IP addresses in the specified ACL or prefix list. • **match ip peer** *acl-id* – Matches on the peer router IP addresses in the specified list. • **match ipv6 address** {*acl-id* | *prefix-list list-name*} – Matches on the route IP addresses in the specified ACL or prefix list. • **match ipv6 next-hop** {*acl-id* | **prefix-list** *list-name* | *ipv6-addr*} – Matches on the next-hop router IP addresses in the specified ACL or prefix list, or the specified IPv6 address. • **match ipv6 peer** *acl-id* **[exact-match]**– Matches on the BGP communities listed in the specified large community list. • **match large community***list-id* **[exact-match]**– Matches on the BGP communities listed in the specified large community list. • **match local-preference** *num* – Matches on the specified local preference value, 0-4294967295. • **match metric** *num* – Matches on the specified route metric value, 0-4294967295. • **match origin** {**egp** | **igp** | **incomplete**} – Matches on the specified BGP origin code. • **match route-type external** {**type-1** | **type-2**} –

Command	Description
	Matches on the specified external route type. • **match scaleout** *cluster-id* – Matches on the specified scaleout status. • **match tag** *tag-value* – Matches on the specified TAG value, 0-4294967295.
set *attribute*	Sets information for matching routes: • **set aggregator as** *as-num ipaddr* – Sets the aggregator attribute. • **set as-path prepend** *as-num* [...]– Adds the specified BGP AS number(s) to the front of the AS-path attribute. • **set atomic-aggregate** – Specifies that a BGP route has been aggregated, and that path information for the individual routes that were aggregated together is not available. • **set comm-list** *list-id* **delete** – Sets the specified BGP community list to be deleted. • **set community** *community-value* – Sets the BGP community ID to the specified value: ◦ <*1-4294967295*> – Sets the community number. ◦ *AS*:*NN*, where *AS* is the AS number and *NN* is a numeric value in the range 1-4294967295. ◦ **internet** – Internet route. ◦ **local-AS** – Advertises routes only within the local Autonomous System (AS), not to external BGP peers. ◦ **no-advertise** – Does not advertise routes. ◦ **no-export** – Does not advertise routes outside the AS boundary.

Command	Description
	◦ **none** – No community attribute. • **set dampening** [*reachability-half-life* [*reuse-value* [*suppress-value*] [*max-duration* [*unreachability-half-life*]]]] – Enables route-flap dampening. Route-flap dampening helps minimize network instability caused by unstable routes. • *reachability-half-life* – Reachability half life, 1-45 minutes. After a route remains reachable for this period of time, the penalty value for that route is divided in half. The default is 15 minutes. • *reuse-value* [*suppress-value*] – Penalty thresholds for the suppression and reuse (re-advertisement) of a route. The supported range for each value is 1-20000. The default *suppress-value* is 2000. the default *reuse-value* is 750. • *max-duration* – Maximum amount of time a route will remain suppressed, 1-255 minutes. The default is 4 times the *reachability-half-life*. • *unreachability-half-life* – *Un*reachability half life, 1-45 minutes. After a route remains unreachable for this period of time, the penalty value for that route is divided in half. (cont.)
set *attribute*	• **set extcommunity** *comm-id* [...]– Sets the BGP extended community attribute. • **set ip next-hop** *ipaddr* – Sets the next hop for matching IPv4 routes. • **set ipv6** [**local**] *ipv6addr* – Set the next hop for matching IPv6 routes. If the address is for an inside network (not globally routable), use the **local** option.

Command	Description
	• **set large-comm-list** *list-id* **delete**– Sets the specified BGP large community list to be deleted. • **set large-community** *community-value*– Sets the BGP Large community ID to the specified value: ◦ **NAME<length:1-128>** – Sets the large community number in the xx:yy:zz format. ◦ **none** – No community attribute. • **set level** {**level-1** | **level-1-2** | **level-2**} – Sets the IS-IS level for exporting a route to IS-IS. • **set local-preference** *num* – Sets the BGP local preference path attribute. • **set metric** *metric-value* – Sets the metric value for the destination routing protocol. • **set metric-type** {**external** | **internal** | **type-1** | **type-2**} – Sets the metric type for the destination routing protocol. • **set origin** {**egp** | **igp** | **incomplete**} – Sets the origin attribute: ◦ **egp** – Exterior gateway protocol. ◦ **igp** – Interior gateway protocol. ◦ **incomplete** – Unknown heritage. • **set originator-id** *ipaddr* – Sets the BGP originator attribute. • **set tag** *tag-value* – Sets the tag value for the destination routing protocol. • **set weight** *num* – Sets the BGP weight value for the routing table.

Default None

Mode Configuration mode

Usage For options that use an ACL, the ACL must use a permit action. Otherwise, the route map action is deny.

router

Description Enter the configuration mode for a dynamic routing protocol.

Syntax

```
[no] router protocol
```

Replace *protocol* with one of the following:

Command	Description
bgp *AS-num*	Specifies an Autonomous System (AS) for which to run Border Gateway Protocol (BGP) on the ACOS device. This also enters BGP configuration mode.
ipv6 {**ospf** [*tag*] | **rip**}	Specifies an IPv6 OSPFv3 process (1-65535) or Routing Information Protocol (RIP) process to run on the IPv6 link, and also enter configuration mode for the specified protocol.
isis [*tag*]	Enter configuration mode for Intermediate System to Intermediate System (IS-IS).
ospf [*process-id*]	Specifies an IPv4 OSPFv2 process (1-65535) to run on the ACOS device, and also enter OSPF configuration mode.
rip	Enter configuration mode for Routing Information Protocol (RIP).

Default Dynamic routing protocols are disabled by default.

Mode Configuration mode

Usage This command is valid only when the ACOS device is configured for gateway mode (Layer 3).

Example The following command enters the configuration level for OSPFv2 process 1:

```
ACOS(config)# router ospf 1
ACOS(config-ospf:1)#
```

router log file

Description Configure router logging to a local file.

Syntax

```
[no] router log file
{name string | per-protocol | rotate num | size Mbytes}
```

Parameter	Description
name *string*	Name of the log file.
per-protocol	Uses separate log files for each protocol. Without this option, log messages for all protocols are written to the same file. By default, this is disabled.
rotate *num*	Specifies the number of backups to allow for each log file. When a log file becomes full, the logs are saved to a backup file and the log file is cleared for new logs. You can specify 0-100 backups. If the maximum number of backups is reached, the oldest backups are purged to make way for new ones. The default is 0.
size *Mbytes*	Specifies the size of each log file. You can specify 0-1000000 Mbytes. If you specify 0, the file size is unlimited. The default size is 0.

Mode Configuration mode

Usage When you enable logging, the default minimum severity level that is logged is debugging.

This command is independent of the router log log-buffer command, and enabling or disabling the router log log-buffer command does not affect its usage. When configured, use show router log file to display router logs.

The **per-protocol** option is recommended. Without this option, messages from all routing protocols will be written to the same file, which may make troubleshooting more difficult.

router log log-buffer

Description Sends router logs to the logging buffer.

Syntax

```
[no] router log log-buffer
```

Default Enabled

Mode Configuration mode

Usage Use show log to display entries for this command. This configuration is independent from router log file and enabling or disabling `router log log-buffer` has no effect on router log file configuration.

run-hw-diag

Description Access the hardware diagnostics menu on the next reboot.

NOTE:

- The system will be unavailable for normal operations while a test is running.
- A reboot is required before the hardware diagnostics menu appears. If you reboot to a software release that does not support the hardware diagnostics menu, the menu is not available.

Syntax

```
run-hw-diag
```

Mode Configuration mode

Usage The hardware diagnostic menu is available only on serial console sessions. To run a test, you must use a serial console connection.

The **run-hw-diag** command requires a reboot. After the reboot is completed, a menu with the following options appears:

- 1 - Memory Test
- 2 - HDD/CF Scan Test (1-2 hours)
- 3 - MBR (Master Boot Record) check

- 4 - Complete Test (all above)
- x - Reboot

NOTE: As indicated in the description for option 2, the media scan test, the test takes *1-2 hours to complete*.

After a test is completed, you can use the x option to reboot. If you do not enter an option to run another test or reboot, the system automatically reboots after 5 minutes. The same software image that was running when you entered the **run-hw-diag** command is reloaded during the reboot.

Example The following example shows how to access the hardware diagnostic menu:

```
ACOS(config)# run-hw-diag
Please confirm: You want to run HW diagnostics (N/Y)?:y
Please reboot the system when you are ready.
HW diagnostic will run when the system comes back up.
ACOS(config)# end
ACOS# reboot
Proceed with reboot? [yes/no]:yes
Rebooting......
INIT: version 2.86 booting
Booting.........mdadm: stopped /dev/md1
mdadm: stopped /dev/md0


                  00000000000
-------------------------------------------------------
|      Hardware Diagnostic Menu                       |
-------------------------------------------------------
|  1 - Memory Test                                    |
|  2 - HDD/CF Scan Test (1-2 hours)                   |
|  3 - MBR (Master Boot Record) check                 |
|  4 - Complete Test (all above)                      |
|  x - Reboot                                         |
-------------------------------------------------------
Please select an option [1-4, x]:
```

running-config display

Description Configure whether or not aFleX and class-list file information should be included in the running-config.

Syntax

```
[no] running-config display {aflex | class-list}
```

Parameter	Description
aflex	Show aFleX scripts in the running-config.
class-list	Show class-list files in the running-config.

Default By default, aFlex and class-list file information is not displayed.

Mode Configuration mode

Usage One or both options may be specified.

session-filter

Description Configures a session filter.

Syntax

```
[no] session-filter filter-name set
{
dest-addr ipv4addr [dest-mask {/length | mask}] |
dest-port portnum |
ipv6 |
sip |
source-addr ipv4addr |
source-port portnum
}
```

Parameter	Description
dest-addr **dest-port** **source-addr** **source-port**	Matches on sessions that have a source or destination IPv4 address or port: • **source-addr***ipaddr* [{*subnet-mask* | **/***mask-length*}] – Matches on IPv4 sessions that have the specified source IP address. • **source-port** *port-num* – Matches on IPv4 sessions that have the specified source protocol port number, 1-65535.

Parameter	Description
	• **dest-addr** – Matches on IPv4 sessions that have the specified destination IP address. • **dest-port** – Matches on IPv4 sessions that have the specified destination protocol port number, 1-65535. You can use one or more of the suboptions together in a single command, nested in the order shown above. For example, if the first suboption you enter is **dest-addr**, the only additional suboption you can specify is **dest-port**.
ipv6	Matches on all sessions that have a source or destination IPv6 address.
sip	Matches on all SIP sessions.

Default No session filters are configured by default.

Mode Configuration mode

Usage Session filters allows you to save session display options for use with the **clear session** and show session commands. Configuring a session filter allows you to specify a given set of options one time rather than re-entering the options each time you use the **clear session** or **show session** command.

Example The following commands configure a session filter and use it to filter **show session** output:

```
ACOS(config)# session-filter f1 source-addr 1.0.4.147
ACOS(config)# show session filter f1
Prot Forward Source          Forward Dest           Reverse
Source          Reverse Dest           Age Hash
-----------------------------------------------------------------
-----------------------------------------
Tcp  1.0.4.147:51613         1.0.100.1:21
1.0.3.148:21           1.0.4.147:51613        120   1
```

sflow

Description Enables the ACOS device to collect information about Ethernet data interfaces and send the data to an external sFlow collector (v5).

Syntax

```
[no] sflow
{
agent address {ipaddr | ipv6addr} |
collector {ip ipaddr | ipv6 ipv6addr} portnum |
polling type |
sampling {ethernet portnum [to portnum] | ve ve-num [to ve-
num]} |
setting sub-options |
source-address {ip ipaddr | ipv6 ipv6addr}
}
```

Parameter	Description
agent address {*ipaddr* | *ipv6addr*}	Configure an sFlow agent. The *ipaddr* value can be any valid IPv4 or IPv6 address. By default, sFlow datagrams use the management IP of the ACOS device as the source address, but you can specify a different IP address, if desired. The information will appear in the Layer 4 information section of the sFlow datagram, and it is not used to make routing decisions.
collector {**ip** *ipaddr* | **ipv6** *ipv6addr*} *portnum*	Configure up to four sFlow collectors. The IP address is that of the sFlow collector device. Specify the port number, with a range from 1-65535. The default port number is 6343.
polling *type*	Enables sFlow export of DDoS Mitigation statistics for the source IP address(es) matched by this rule. You can enable polling for the following types of data: • **cpu-usage** – Polls for CPU utilization statistics. • **ethernet** – Polls for Ethernet data interface statistics. • **http-counter** - Polls for HTTP statistics. • **ve** - Polls for statistics for Virtual Ethernet (VE) interfaces.

Parameter	Description
	All sFlow polling (collection) is disabled by default
sampling {**ethernet** *portnum* [**to** *portnum*] | **ve** *ve-num* [**to** *ve-num*]}	Enable sFlow sampling on a specified interface. There is no default.
setting *sub-options*	Configure global sFlow settings: • **counter-polling-interval** *seconds* – Configure the sFlow counter polling interval. The **interval** *seconds* option specifies the frequency with which statistics for an interface are periodically sampled and sent to the sFlow collector. The range can be configured to a value from 1-200 seconds. The default polling interval is 20 seconds. • **local-collection** – Configure the local sFlow collection. ◦ **enable** – Enable local sFlow collection. ◦ **disable** – Disable local sFlow collection. **NOTE:** The sflow setting local-collection is supported in the shared partition. However, if this command is enabled in the shared partition, it is also enabled in the private partition regardless of the default setting. • **max-header** *bytes* – Maximum number of bytes to sample from any given packet, 14-512 bytes. The default is 128 bytes.

Parameter	Description
	• **packet-sampling-rate** *num* – Configure sFlow default packet sampling rate. The *num* option specifies the value of *N*, where *N* is the value of the denominator in the ratio at which a single packet will be sampled from a denominator ranging from 10-1000000. The default is 1000, meaning one packet out of every 1000 will be sampled. • **source-ip-use-mgmt** – Enable use of the management interface's IP as the source address for outbound sFlow packets.
source-address {**ip** *ipaddr* | **ipv6** *ipv6addr*}	Source IP address for sFlow packets sent from ACOS to sFlow collectors. By default, the IP address of the egress interface is used. You can specify a data interface's IP address or the management interface's IP address as the source address for sFlow packets sent to the collector. However, the current release does not support routing of sFlow packets out the management interface. The sFlow collector must be able to reach the ACOS device through a data interface, even if you use the ACOS device's management IP address as the source address of sFlow packets sent to the collector.

Default Described above, where applicable.

Mode Configuration mode

Usage Enable either or both of the following types of data collection, for individual Ethernet data ports:

- Packet flow sampling – ACOS randomly selects incoming packets on the monitored interfaces, and extracts their headers. Each packet flow sample contains the first 128 bytes of the packet, starting from the MAC header. Note that setting a smaller value for the *num* variable increases the sampling frequency, and larger numbers decrease the sampling frequency. This is due to the fact that the variable is in the denominator.

- Counter sampling – ACOS periodically retrieves the send and receive statistics for the monitored interfaces. These are the statistics listed in the Received and Transmitted counter fields in **show interface** output.

Notes

- Sampling of a packet includes information about the incoming interface but not the outgoing interface.
- None of the following are supported:
  - Host resource sampling
  - Application behavior sampling
  - Duplication of traffic to multiple sFlow collectors
  - Configuration of sFlow Agent behavior using SNMP

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following commands specify the sFlow collector, and enables use of the management interface's IP as the source IP for the data samples sent to the sFlow collector:

```
ACOS(config)# sflow collector ip 192.168.100.3 5
ACOS(config)# sflow setting source-ip-use-mgmt
```

smtp

Description Configure a Simple Mail Transfer Protocol (SMTP) server to use for sending emails from the ACOS device.

Syntax

```
[no] smtp parameter
```

Parameters	Description
hostname | *ipaddr*	Configure a name or IP address for the SMTP server.
mailfrom *email-src-addr*	Specifies the email address to use as the sender (From) address.

Parameters	Description
`needauthentication`	Specifies that authentication is required. This is disabled by default.
`port` *`protocol-port`*	Specifies the protocol port on which the server listens for SMTP traffic. The default port is 25.
`server` *`hostname`*	Configure a name for the SMTP server.
`username` *`name`* `password` *`string`*	Specifies the username and password required for access. The password can be 1-31 characters long.

Default No SMTP servers are configured by default. When you configure one, it has the default settings described in the table above.

Mode Configuration mode

Usage The following commands accomplish the same thing:

```
ACOS(config)# smtp MAILSERVER
```

and

```
ACOS(config)# smtp server MAILSERVER
```

Using the `server` keyword is recommended and in some cases, necessary (for example, if you want to configure a server name “mail”; this is not allowed without the `server` keyword because of the conflict with the `mailfrom` CLI option).

Example The following command configures the ACOS device to use SMTP server “MAILSERVER1”:

```
ACOS(config)# smtp server MAILSERVER1
```

snmp-server community

Description Deprecated command to configure an SNMP community string.

Use snmp-server SNMPv1-v2c.

snmp-server contact

Description Configure SNMP contact information.

Syntax

```
[no] snmp-server contact contact-name
```

Replace *contact-name* with the SNMP contact; for example, an E-mail address.

Default Empty string

Mode Configuration mode

Usage The **no** form removes the contact information.

By default, the SNMP sysContact OID value is synchronized among all member ACOS Devices of an aVCS virtual chassis. You can disable this synchronization, on an individual device basis.

NOTE: After configuring this option for an ACOS Device, if you disable aVCS on that device, the running-config is automatically updated to continue using the same sysContact value you specified for the device. You do not need to reconfigure the sysContact on the device after disabling aVCS.

Example The following command defines the SNMP contact with the E-mail address “exampleuser@exampledomain.com”:

```
ACOS(config)# snmp-server contact
exampleuser@exampledomain.com
```

snmp-server disable traps

Description Disable group or all traps in L3V partitions.

Syntax

```
[no] snmp-server disable traps {
  all |
  gslb trap-name |
  slb trap-name |
  slb-change trap-name |
  snmp trap-name |
  vrrp-a trap-name |
}
```

Mode Configuration mode

Usage When this flag is set, user will not able to see any traps from this L3V partition even the traps are enabled in the share partition.

Usage This command will overwrite all the traps enable previous defined.

snmp-server enable schema-agent

Description Enables the SNMP schema agent.

Syntax

```
[no] snmp-server enable schema-agent
```

Default Disabled.

Mode Configuration mode

Usage The schema agent facilitates enhanced SNMP support for Multi-PU platforms by automatically generating SNMP tables for each configuration management (CM) object and enables advanced data fetching mechanisms.

NOTE: For L3V partitions, the SNMP tables do not include a partition index. To request data for an L3V partition, attach the partition name to the community string (e.g., public@p1) in the SNMP request. The response for the request will contain data specific to the requested L3V partition.

snmp-server enable service

Description Enable SNMP service on the ACOS Device.

Syntax

```
[no] snmp-server enable service
```

Default SNMP is disabled by default.

Mode Configuration mode

For security, SNMP is disabled on all data interfaces. Use the enable-management command to enable SNMP on data interfaces.

NOTE: In L3V partition, if SNMP is enabled, user can configure a community string that is used to get requests to the L3V partition and traps send out from this L3V partition.

Example The following commands enable SNMP service:

```
ACOS(config)# snmp-server enable service
ACOS(config)# snmp-server SNMPv1-v2c user u1
ACOS(config0yser:u1)# community read public
```

snmp-server enable traps

Description Enables and specifies traps on the ACOS Device.

Syntax

```
[no] snmp-server enable traps {parameters}
```

Parameter	Description
all	Enables all the traps described below. **NOTE:** The **all** option can be specified at any command level to enable all SNMP traps at that level.
gslb	Enables GSLB group traps: • **group** – Enable group-related traps. • **service-ip** – Enable traps related to service-IPs. • **site** – Enable site-related traps. • **zone** – Enable zone-related traps.
lldp	Enables LLDP group traps.
lsn	Enables LSN group traps: • **fixed-nat-port-mapping-file-change** - Enables LSN

Parameter	Description
	trap when the fixed NAT port mapping file changes). • **per-ip-port-uage-threshold** - Enables LSN trap when IP total port usage reaches the threshold. • **total-port-usage-threshold** - Enables LSN trap when NAT total port usage reaches the threshold. • **traffic-exceeded** - Enables LSN trap when NAT pool reaches the threshold.
network	Enables network group traps: • **trunk-port-threshold** – Indicates that the trunk ports threshold feature has disabled trunk members because the number of up ports in the trunk has fallen below the configured threshold.
routing	Enables the routing group traps: • **bgp** – Enables traps for BGP routing. BGP traps for IPv4 address family as defined in rfc4273: ◦ `bgpEstablishedNotification` - A BGP neighbor transitions to the Established state. ◦ `bgpBackwardTransNotification` - A BGP FSM transitions from a higher state to a lower state for the BGP peer, e.g. from Established to OpenConfirm or from Connect to Idle. BGP traps for IPv4 and IPv6 address families as defined in AX-BGP-MIB proprietary MIB: ◦ `bgp ax` - Enables AX-BGP-MIB traps for IPv4 and IPv6 families: ■ `bgpEstablishedNotification` - A BGP neighbour transitions to the Established state. ■ `bgpBackwardTransNotification` - A BGP FSM transitions from a higher state to a lower state

Parameter	Description
	for the BGP neighbour. ■ bgpPrefixThresholdExceededNotification - The prefix count exceeds the threshold limit configured for IPv4 or IPv6 peer. ■ bgpPrefixThresholdClearNotification - The prefix count drops below the warning threshold configured for the IPv4 or IPv6 peer if it has exceeded the threshold before. • **isis** – Enables traps for IS-IS routing: ◦ isisAdjancencyChange ◦ isisAreaMismatch ◦ isisAttemptToExceedMaxSequence ◦ isisAuthenticationFailure ◦ isisAuthenticationTypeFailure ◦ isisCorruptedLSPDetected ◦ isisDatabaseOverload ◦ isisIDLenMismatch ◦ isisLSPTooLargeToPropagate ◦ isisManualAddressDrops ◦ isisMaxAreaAddressesMismatch ◦ isisOriginatingLSPBufferSizeMismatch ◦ isisOwnLSPPurge ◦ isisProtocolsSupportedMismatch ◦ isisRejectedAdjacency ◦ isisSequenceNumberSkip ◦ isisVersionSkew • **ospf**– Enables traps for OSPF routing:

Parameter	Description
	◦ ospfIfAuthFailure ◦ ospfIfConfigError ◦ ospfIfRxBadPacket ◦ ospfIfStateChange ◦ ospfLsdbApproachingOverflow ◦ ospfLsdbOverflow ◦ ospfMaxAgeLsa ◦ ospfNbrStateChange ◦ ospfOriginateLsa ◦ ospfTxRetransmit ◦ ospfVirtIfAuthFailure ◦ ospfVirtIfConfigError ◦ ospfVirtIfRxBadPacket ◦ ospfVirtIfStateChange ◦ ospfVirtIfTxRetransmit ◦ ospfVirtNbrStateChange
scaleout	Enables the Scaleout group traps: • **infrastructure** – Enables Infrastructure group traps: ◦ all – Enables all the infrastructure traps. ◦ cluster – Enables cluster group traps. ■ election – Enables election status trap. ■ master-calling-re-election – Enables re-election trap. ■ node-status – Enables active node status trap. ◦ master-node – Enables master node group traps.

Parameter	Description
	■ `traffic-map-distribution` – Enables Traffic-map distribution trap. ■ `vserver-traffic-map-update` – Enables vServer Traffic-map trap. ○ `service-node` – Enables service node group traps. ■ `local-device-disabled` – Enables local device disabled trap. ■ `service-master` – Enables service-master trap. ■ `traffic-map-update` – Enables traffic map update trap.
slb	Enables the SLB group traps: • **application-buffer-limit** – Indicates that the configured SLB application buffer threshold has been exceeded. • **bw-rate-limit-exceed** – Indicates that the bw-rate-limit is exceeded by either a real server or a real port or both. • **bw-rate-limit-resume** – Indicates that the bw-rate-limit has fallen below the resume threshold after transitioning from 'exceed' threshold state for either real server or real port or both. • **gateway-down** – Enable gateway down trap only. • **gateway-up** – Enable gateway up trap only. • **server-conn-limit** – Indicates that an SLB server has reached its configured connection limit. • **server-conn-resume** – Indicates that an SLB server has reached its configured connection-resume value. • **server-disabled** – Indicates that an SLB server has been disabled.

Parameter	Description
	• **server-down** – Indicates that an SLB server has gone down. • **server-selection-failure** – Indicates that SLB was unable to select a real server for a request. • **server-up** – Indicates that an SLB server has come up. • **service-conn-limit** – Indicates that an SLB service has reached its configured connection limit. • **service-conn-resume** – Indicates that an SLB service has reached its configured connection-resume value. • **service-down** – Indicates that an SLB service has gone down. • **service-group-down** – Indicates that an SLB service group has gone down. • **service-group-member-down** – Indicates that an SLB service group member has gone down. • **service-group-member-up** – Indicates an SLB service group member has come up. • **service-group-up** – Indicates that an SLB service group has come up. • **service-up** – Indicates that an SLB service has come up.
slb (cont.)	• **vip-connlimit** – Indicates that the connection limit configured on a virtual server has been exceeded. • **vip-connratelimit** – Indicates that the connection rate limit configured on a virtual server has been exceeded. • **vip-down** – Indicates that an SLB virtual server has gone down. • **vip-port-connlimit** – Indicates that the connection

Parameter	Description
	limit configured on a virtual port has been exceeded. • **vip-port-connratelimit** – Indicates that the connection rate limit configured on a virtual port has been exceeded. • **vip-port-down** – Indicates that an SLB virtual service port has gone down. • **vip-port-qps** – Indicates that the QPS value exceeds the configured high threshold, drops below the configured low threshold, or returns to a normal level. • **vip-port-up** – Indicates that an SLB virtual service port has come up. An SLB virtual server's service port is up when at least one member (real server and real port) in the service group bound to the virtual port is up. • **vip-up** – Indicates that an SLB virtual server has come up.
slb-change	Enables the SLB change traps: • **connection-resource-event** - Enables system connection resource event trap. • **resource-usage-warning** – Indicates resource usage threshold met. • **server** – Indicates a real server was created or deleted. • **server-port** – Indicates a real server port was created or deleted. • **ssl-cert-change** – Indicates that an SSL certificate has been changed. • **ssl-cert-expire** – Indicates that an SSL certificate has expired.

Parameter	Description
	• **system-threshold** – Indicates that the device has exceeded the Usage threshold for a specified SLB resource. • **vip** – Indicates a virtual server was created or deleted. • **vip-port** – Indicates a virtual service port was created or deleted.
snmp	Enables SNMP group traps: • **linkdown** – Indicates that an Ethernet interface has gone down. • **linkup** – Indicates that an Ethernet interface has come up.
system	Enables the system group traps: • **all** - Enables all system group traps. • **apps-global** - Enables apps-global group traps. ◦ **cps-threshold** - Enables Connection per second (CPS) trap. ◦ **sessions-threshold** - Enables number of sessions threshold trap. • **control-cpu-high** – Indicates that the control CPU utilization is higher than the configured threshold. • **data-cpu-high** – Indicates that data CPU utilization is higher than the configured threshold. • **fan** – Indicates that a system fan has failed. Contact A10 Networks, Inc.. • **file-sys-read-only** – Indicates that the file system has entered read-only mode. • **high-disk-use** – Enables system high disk usage traps.

Parameter	Description
	• **high-memory-use** – Indicates that the memory usage on the ACOS Device is higher than the configured threshold. • **high-temp** – Indicates that the temperature inside the ACOS device is higher than the configured threshold. • **license-management** – Enables license management traps. • **low-temp** – Enables system low temperature trap. • **packet-drop** – Indicates that the number of dropped packets during the previous 10-second interval exceeded the configured threshold. **NOTE:** This trap is not applicable to some device types. The trap is applicable to Thunder Series hardware-based models and software-based models. • **power** – Indicates that a power supply has failed. Contact A10 Networks, Inc.. • **pri-disk** – Indicates that the primary Hard Disk has failed or the RAID system has failed. In dual-disk models, the primary Hard Disk is the one on the left, as you are facing the front of the ACOS Device. • **restart** – Indicates that the ACOS Device is going to reboot or reload. • **sec-disk** – Indicates that the secondary Hard Disk has failed or the RAID system has failed. The secondary Hard Disk is the one on the right, as you are facing the front of the ACOS Device. **NOTE:** This trap applies only to models that use disk drives.

Parameter	Description
	• **shutdown** – Indicates that the ACOS Device has shut down. • **smp-resource-event** – Enables system smp resource event trap. • **start** – Indicates that the ACOS Device has started. • **syslog-severity-one** - Enables system syslog severity one message trap. • **tacacs-server-up-down** - Enables system TACACS monitor server is up or down trap.
vcs state-change	Enable the VCS state-change trap.
vrrp-a	Enables VRRP-A high availability traps: **active** - Indicates a device has become the active device. **standby** - Indicated a device bas become the standby device.

NOTE: In L3V partitions, only the **all**, **slb**, **gslb**, **slb-change**, **snmp**, and **vrrp-a** traps are available.

Default SNMP service is disabled by default.

Mode Configuration mode

Usage For security, SNMP and SNMP trap are disabled on all data interfaces. Use the **enable-management** command to enable SNMP on data interfaces.

The **no** form disables traps.

If the ACOS Device is a member of an aVCS virtual chassis platform, use the **device-context** command to specify the device in the chassis to which this command must apply. This is only valid for SNMP routing

(**snmp-server enable traps routing** *trap-name*) and network (**snmp-server enable traps network** *trap-name*) traps.

Example The following command enables all traps:

```
ACOS(config)# snmp-server enable traps all
```

Example The following command enables all SLB traps:

```
ACOS(config)# snmp-server enable traps slb all
```

Example The following commands enable SLB traps server-conn-limit and server-conn-resume:

```
ACOS(config)# snmp-server enable traps slb server-conn-limit
ACOS(config)# snmp-server enable traps slb server-conn-resume
```

Example The following commands enable SLB traps server-conn-limit and server-conn-resume:

```
ACOS(config)# snmp-server enable traps slb server-conn-limit
ACOS(config)# snmp-server enable traps slb server-conn-resume
```

Example The following commands enable BGP AX routing traps:

```
ACOS(config)# snmp-server enable traps routing bgp ax
bgpEstablishedNotification
ACOS(config)# snmp-server enable traps routing bgp ax
bgpBackwardTransNotification
ACOS(config)# snmp-server enable traps routing bgp ax
bgpPrefixThresholdExceededNotification
ACOS(config)# snmp-server enable traps routing bgp ax
bgpPrefixThresholdClearNotification
```

Example The following commands enable apps-global group traps:

```
ACOS(config)# snmp-server enable traps system apps-global cps-
threshold
ACOS(config)# snmp-server enable traps system apps-global
sessions-threshold
```

Example The following command enables trap on ISIS routing protocol to send a notification when a Link State PDU (LSP) is received with a parse error:

```
ACOS(config)# snmp-server enable traps routing isis
isisLSPErrorDetected
```

Example The following command enables all Scaleout infrastructure traps:

```
ACOS(config)# snmp-server enable traps scaleout infrastructure
all
```

Related Commands:

- enable-management
- monitor
- system apps-global

snmp-server engineID

Description Set the SNMPv3 engine ID of this ACOS Device.

Prerequisite The snmp-server service should be enabled for this ACOS device.

Syntax

```
[no] snmp-server engineID hex-string
```

Parameter	Description
hex-string	Specifies local engineID (10-24 characters). REQUIRED. Alphanumeric
|	OPTIONAL. Alphabetic. Specifies output modifiers.

Mode Global Configuration

Example The following command sets SNMP engineID:

```
ACOS#snmp-server engineID 80001f8804393837
```

Related Commands:

- snmp-server enable service

snmp-server group

Description Configure an SNMP group for SNMPv3.

Syntax

```
[no] snmp-server group group-name v3
{auth | noauth | priv} read view-name
```

Parameter	Description
group-name	Specifies the name of the SNMP group.
auth	Uses packet authentication but does not encrypt the packets. (This is the authNoPriv security level.)
noauth	Does not use any authentication of packets. (This is the noAuthNoPriv security level.)
priv	Uses packet authentication and encryption. (This is the authPriv security level.)
read *view-name*	Specifies the name of a read-only view for accessing the MIB object values. Views are created using the snmp-server view command.

Default The configuration does not have any default SNMP groups.

Mode Configuration mode

Example The following commands add SNMP v3 group “group1” with authPriv security and read-only view “view1”:

```
ACOS(config)# snmp-server group group1 v3 priv read view1
```

snmp-server host

Description Configure an SNMP v1/v2c trap receiver.

Syntax

```
[no] snmp-server host {parameters}
```

Parameter	Description
trap-receiver	Hostname or IP address of the remote device to which traps will be sent.
version {v1 | v2c | v3}	SNMP version. If you omit this option, the trap receiver can use SNMP v1 or v2c.
community-string	Community string for the v1 or v2c traps.
user name	SNMP v3 user name for sending the traps.
udp-port *port-num*	UDP port to which the ACOS Device sends the trap.

Default No SNMP hosts are defined. When you configure one, the default SNMP version is v2c and the default UDP port is 162.

Mode Configuration mode

Usage You can configure up to 16 trap receivers.

The “no” form removes the trap receiver.

Example The following command configures SNMP trap receiver 100.10.10.12 to use community string “public” and UDP port 166 for SNMP v2c traps.

```
ACOS(config)# snmp-server host 100.10.10.12 version v2c public
udp-port 166
```

snmp-server location

Description Configure SNMP location information.

Syntax

```
[no] snmp-server location location
```

Replace *location* with the location of the ACOS Device.

Default Empty string

Mode Configuration mode

Example The following command configures the location as “ExampleLocation”:

```
ACOS(config)# snmp-server location ExampleLocation
```

snmp-server management-index

Description Define index of management interface.

Syntax

```
[no] snmp-server management-index num
```

Default N/A

Mode Configuration mode

snmp-server slb-data-cache-timeout

Description Configure the SLB data cache timeout.

Syntax

```
[no] snmp-server slb-data-cache-timeout seconds
```

Replace *seconds* with the number of seconds (5-120) of the SLB data cache timeout.

Default 60 seconds.

Mode Configuration mode

Example The following example sets the SLB data cache timeout to 45 seconds.

```
ACOS(config)# snmp-server slb-data-cache-timeout 45
```

snmp-server SNMPv1-v2c

Description Define an SNMPv1 or SNMPv2c community. The members of the community can gain access to the SNMP data available on this device.

Syntax

```
[no] snmp-server SNMPv1-v2c user user-name {community | oid | remote}
```

This command changes the CLI to an SNMP community configuration mode, where the following commands are available:

Parameter	Description
`community read {string | encrypted}`	Define a community string with the following options: • *string* - Define the value of the community string. • `encrypted` - Define the community string with an encrypted password. Do NOT use this option manually.
`oid` *oid-value*	Object ID. This option restricts the objects that the ACOS Device returns in response to GET requests. Values are returned only for the objects within or under the specified OID.
`remote {` *ipv4addr* `[/mask-length | mask] |` *ipv6addr* `|` *DNS-remote-host* `}`	Restricts SNMP access to a specific remote host or subnet. When you use this option, only the specified host or subnet can receive SNMP data from the ACOS Device by sending a GET request to this community.

NOTE: The `oid` and `remote` parameters are not available in the L3V partition. They are only applicable in the shared partition.

Mode The configuration does not have any default SNMP communities.

Mode Global configuration mode

Usage All SNMP communities are read-only. Read-write communities are not supported. The OID for A10 Thunder Series objects is 1.3.6.1.4.1.22610.

Example The following commands enable SNMP and define community string "a10community":

```
ACOS(config)# snmp-server enable service
ACOS(config)# snmp-server SNMPv1-v2c user u1
ACOS(config-user:u1)# community read a10community
ACOS(config-user:u1)# remote 10.10.10.0 /24
ACOS(config-user:u1)# remote 20.20.20.0 /24
ACOS(config-user:u1)# oid 1.2.3
ACOS(config-user:u1-oid:1.2.3)# remote 30.30.30.0 /24
ACOS(config-user:u1-oid:1.2.3)# remote 40.40.40.0 /24
```

Hosts in 10.10.10.0 /24 and 20.20.20.0 /24 can access the entire MIB tree using the "a10community" community string. Hosts in 30.30.30.0 /24 and 40.40.40.0 /24 can access the MIB sub-tree 1.2.3 using the community string "a10community."

Example The following example deletes the OID sub-tree 1.2.3:

```
ACOS(config-user:u1)# no oid 1.2.3
```

snmp-server SNMPv3

Description Define an SNMPv3 user.

NOTE: The old **snmp-server user** command is deprecated, instead use this command to configure an SNMPv3 user.

Syntax

```
[no] snmp-server SNMPv3 user username group groupname v3
{auth {md5 | sha| sha-512| sha-384| sha-256| sha-224} {string
| encrypted} auth-password [priv {des | aes| aes-192| aes-256}
priv-password] |
 noauth
}
```

Parameter	Description
username	Specifies the SNMP user name.
groupname	Specifies the group to which the SNMP user belongs.
v3	Specifies SNMP version 3.
{auth {md5 | sha| sha-512| sha-384| sha-256| sha-224} {*string* | encrypted}	Specifies the encryption method to use for user authentication. • md5 - Uses Message Digest Algorithm 5 (MD5) for authentication. • sha - Uses Security Hash Algorithm (SHA) for authentication. • sha-512 - Uses SHA with key size of 512 bits for authentication. • sha-384 - Uses SHA with key size of 384 bits for authentication. • sha-256 - Uses SHA with key size of 256 bits for authentication. • sha-224 - Uses SHA with key size of 224 bits for authentication. • The sub-options for authentication are as follows: • *string* - Define the value of the community string. • encrypted - Define the community string with an encrypted password. Do NOT use this option manually.
auth-password	Password for user authentication.
priv {des | aes| aes-192| aes-256}	Specifies the encryption method to use for user privacy. • aes - Uses Advanced Encryption Standard (AES) algorithm. This uses a

Parameter	Description
	fixed block size of 128 bits. AES encryption supersedes DES encryption. • `aes-192` - Uses AES algorithm with key size of 192 bits for encryption. • `aes-256` - Uses AES algorithm with key size of 256 bits for encryption. • `des` - Uses Data Encryption Standard (DES) algorithm to apply a 56-bit key to each 64-bit block of data. This is considered strong encryption.
priv-password	Password for message encryption and privacy (8-31 characters).
noauth	Does not use message encryption or privacy.

Default No SNMP users are configured by default.

Mode Configuration mode

Usage SNMPv3 enables you to configure each user with a name, authentication type with an associated key, and privacy type with an associated key.

- Authentication (**auth**) is performed by using the user's authentication key to sign the message being sent. This can be done using either MD5 or SHA encryption; the authentication key is generated using the specified encryption method and the specified `auth-password`.
- Encryption (`priv`) is performed by using a user's privacy key to encrypt the data portion of the message being sent. This can be done using either AES or DES encryption; the authentication key is generated using the specified encryption method and the specified *priv-password*.

Example The following example shows how to configure SNMPv3 user authentication and encryption where an **exampleuser** is a member of

an **examplegroup**. Authentication using SHA-512 for **authpassword** is configured, along with message encryption using AES-192 or **privpassword**.

```
ACOS(config)# snmp-server enable service
ACOS(config)# snmp-server view exampleview 1.2.3 included
ACOS(config)# snmp-server group examplegroup v3 auth read
exampleview
ACOS(config)# snmp-server SNMPv3 user exampleuser group
examplegroup v3 auth sha-512
ACOS(config)# snmp-server SNMPv3 user exampleuser group
examplegroup v3 auth sha-512 authpassword priv aes-192
privpassword
```

snmp-server table-timeout

Description Configure the table timeout for retrieving MIB table statistics (IF-MIB).

NOTE: Currently, only ifTable (.1.3.6.1.2.1.2.2...) and ifXTable (.1.3.6.1.2.1.31.1.1...) MIB tables are supported.

Prerequisite The snmp-server service should be enabled.

Syntax

```
[no] snmp-server table-timeout [tablename | oid] timeout value
```

Parameter	Description
[*tablename* | *oid*]	Specifies the table name or OID. You can specify a string of 1-128 characters.
timeout value	Specifies the length of time (in seconds) that the table statistics is cached. You can specify 1-60 seconds. The default value is 60 seconds.

Mode Global configuration

Usage If you set the ifTable cache timeout to 5 seconds, then the SNMP queries every 5 seconds to retrieve the table data or counters from the backend.

When SNMP queries within the cache time, the same data shall be retrieved. When the SNMP queries after the cache time, the fresh data is retrieved, and the cache timestamp is updated.

NOTE: Lowering the cache timeout setting causes more SNMP queries and may have an impact on the performance.

Example The following command sets the table-timeout for ifTable:

```
ACOS#snmp-server table-timeout ifTable 10
```

snmp-server view

Description Configure an SNMP view.

Syntax

```
[no] snmp-server view view-name oid {oid-mask | included | excluded}
```

Parameter	Description
view-name	Name of the SNMP view.
oid	MIB family name or OID.
oid-mask	OID mask. Use hex octets, separated by a dot (.) character.
included	MIB family is included in the view.
excluded	MIB family is excluded from the view.

Default N/A

Mode Configuration mode

Usage The OID for ACOS Devices is 1.3.6.1.4.1.22610.

Example The following command adds SNMP view “view1” and includes all objects in the 1.3.6 tree:

```
ACOS(config)# snmp-server view view1 1.3.6 included
```

so-counters

Description Show scale out statistics.

Syntax

```
so-counters [sampling-enable options]
```

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
`all`	All packets.
`so_pkts_conn_in`	Total packets processed for an established connection.
`so_pkts_conn_ redirect`	Total packets redirected for an established connection.
`so_pkts_dropped`	Total packets dropped.
`so_pkts_errors`	Total packet errors.
`so_pkts_in`	Total number of incoming packets.
`so_pkts_new_conn_in`	Total packets processed for a new connection.
`so_pkts_new_conn_ redirect`	Total packets redirected for a new connection.
`so_pkts_out`	Total number of packets sent out.
`so_pkts_redirect`	Total number of packets redirected.
`so_pkts_conn_sync_fail`	Total number of connection sync failures.
`so_pkts_nat_reserve_ fail`	Total number of NAT reserve failures.
`so_pkts_nat_release_ fai`	Total number of NAT release failures.
`so_pkts_conn_l7_sync`	Total number of Layer 7 connection syncs.
`so_pkts_conn_l4_sync`	Total number of Layer 4 connection syncs.
`so_pkts_conn_nat_sync`	Total number of NAT connection syncs.
`so_pkts_redirect_conn_ aged_out`	Total number of redirect connections aged out.

Mode Configuration mode

ssh-login-grace-time

Description Period of time in seconds after a user connects to the ACOS device, but before the user is authenticated.

Configuring a shorter grace period reduces the chance that a malicious user could successfully execute a brute force attack against the SSH server. Such an attack could compromise the device, allowing miscreants to gain root access, install malware, or perhaps even remove the ACOS device from service.

However, the grace period should be set to give users a reasonable amount of time to enter a password, become authenticated, and to establish a secure connection before the ACOS device terminates the connection.

Syntax

```
[no] ssh-login-grace-time seconds
```

Parameter	Description
seconds	SSH login grace time, in seconds (5-600).

Default This feature is enabled by default; the default grace period is 120 seconds (2 minutes). This grace period does not apply to Telnet sessions; only SSH sessions.

Mode Global configuration

Usage Configuring a shorter grace period reduces the chance that a malicious user could successfully execute a brute force attack against the SSH server. Such an attack could compromise the device, allowing miscreants to gain root access, install malware, or perhaps even remove the ACOS device from service.

However, the grace period should be set to give users a reasonable amount of time to enter a password, become authenticated, and to establish a secure connection before the ACOS device terminates the connection.

This command is only available in the shared partition.

In aVCS configurations, this command only applies to the local device.

sshd

Description Perform an SSHD operation on the system.

Syntax

```
sshd
{
key generate [size {2048 | 4096}] |
key load [use-mgmt-port] url |
key regenerate [size {2048 | 4096}] |
key wipe |
re-add-rsa |
restart
}
```

Parameter	Description
key generate [size {2048 | 4096}]	Generate an SSH key. You can choose to specify a key size: • **size 2048** - To generate a 2048-bit key. • **size 4096** - To generate a 4096-bit key.
key load [use-mgmt-port] *url*	Load an SSH key. Specify **use-mgmt-port** to use the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the ACOS device attempts to use the data route table to reach the remote device through a data interface. Specify the *url* to the SSH key. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: • tftp://*host*/*file* • ftp://[*user*@]*host*[*port*:]/*file* • scp://[*user*@]*host*/*file*

Parameter	Description
	• sftp://[user@]host/file
key regenerate	Wipe and regenerate an SSH key. You can choose to specify a key size: • **size 2048** to generate a 2048-bit key • **size 4096** to generate a 4096-bit key.
key wipe	Wipe an SSH key.
re-add-rsa	Remove the SSH public key of a particular IP address/host from the ACOS. Import may fail when the server's SSH key is changed. In such case, you use this command.
restart	Restart the SSH service.

Mode Configuration mode

Example The following example generates the 2048 bit key.

```
ACOS(config)# sshd key generate size 2048
```

syn-cookie

Description Enable hardware-based SYN cookies, which protect against TCP SYN flood attacks.

Syntax

```
[no] syn-cookie enable [on-threshold num off-threshold num]
```

Parameter	Description
on-threshold *num*	Maximum number of concurrent half-open TCP connections allowed on the ACOS device, before SYN cookies are enabled. If the number of half-open TCP connections exceeds the on-threshold, the ACOS device enables SYN cookies. You can specify 0-2147483647 half-open connections.
off-threshold	Minimum number of concurrent half-open TCP connections for which to keep SYN cookies enabled.

Parameter	Description
num	If the number of half-open TCP connections falls below this level, SYN cookies are disabled. You can specify 0-2147483647 half-open connections.

NOTE: It may take up to 10 milliseconds for the ACOS device to detect and respond to crossover of either threshold.

Default Hardware-based SYN cookies are disabled by default. When the feature is enabled, there are no default settings for the on and off thresholds.

Mode Configuration mode

Usage Hardware-based SYN cookies are available only on some models.

If both hardware-based and software-based SYN cookies are enabled, only hardware-based SYN cookies are used. You can leave software-based SYN cookies enabled but they are not used. (Software-based SYN cookies are enabled at the virtual port level using the **syn-cookie enable** command.)

If you omit the **on-threshold** and **off-threshold** options, SYN cookies are enabled and are always on regardless of the number of half-open TCP connections present on the ACOS device.

This command globally enables SYN cookie support for SLB and also enables SYN cookie support for Layer 2/3 traffic. No additional configuration is required for SLB SYN cookie support. However, to use Layer 2/3 SYN cookie support, you also must enable it at the configuration level for individual interfaces.

If L3V partitions are configured, hardware-based SYN cookies must be enabled per individual partition. Hardware-based SYN cookies are NOT partition-aware.

On FTA models only, it is recommended not to use hardware-based SYN cookies if DSR also is enabled. If both features are enabled, a client who sends TCP requests to a VIP that is configured for DSR will receive two SYN-ACKS, one from the ACOS hardware-based SYN-cookie feature, and

the other from the server. This can be confusing to a client because the client expects only one SYN-ACK in reply to the client's SYN.

Example The following command enables hardware-based SYN cookies:

```
ACOS(config)# syn-cookie enable
```

The command in the following example configures dynamic SYN cookies when the number of concurrent half-open TCP connections exceeds 50000, and disables SYN cookies when the number falls below 30000:

```
ACOS(config)# syn-cookie enable on-threshold 50000 off-
threshold 30000
```

Related Commands:

- ip tcp syn-cookie threshold

system

system all-vlan-limit

Description Set the global traffic limits for all VLANs.

The limit applies system-wide to all VLANs; collectively, all ACOS device VLANs cannot exceed the specified limit.

To configure the limit per individual VLAN, use system per-vlan-limit.

Syntax

```
[no] system all-vlan-limit
{bcast | ipmcast | mcast | unknown-ucast} num
```

Parameter	Description
all-vlan-limit	Limit applies system-wide to all VLANs. Collectively, all the ACOS device's VLANs together cannot exceed the specified limit.
per-vlan-limit	Limit applies to each VLAN. No individual can exceed the specified limit.
bast	Limit broadcast traffic.
ipmcast	Limit IP multicast traffic.
mcast	Limit all multicast packets except for IP multicast

Parameter	Description
	packets.
unknown-ucast	Limit all unknown unicast traffic.
num	Specifies the maximum number of packets per second that are allowed of the specified traffic type.

Default 5000 packets per second.

Mode Configuration mode

Example The following command limits each VLAN to 1000 multicast packets per second:

```
ACOS(config)# system per-vlan-limit mcast 1000
```

Related Commands:

- system per-vlan-limit

system anomaly log

Description Enable logging for packet anomaly events. This type of logging applies to system-wide attacks such as SYN attacks.

Syntax

```
[no] system anomaly log
```

Default Disabled

Mode Configuration mode

system apps-global

Description Configures global or generic settings for the application.

Syntax

```
[no] system apps-global{cps-threshold num | log-session-on-established | msl-time seconds | sessions-threshold num | timer-wheel-walk-limit num}
```

Option	Description
cps-	Sets a value for the system-wide Connections Per

Option	Description
threshold *num*	Second (CPS) threshold. A trap and a log is generated when the following events occur: • CPS in the system exceeds the configured threshold. • CPS in the system subsequently subceeds the configured threshold. The CPS is computed as the sum total of the values of l4_cps, l7_cps, l7_tps, ssl_cps, ServSSLcpi, ip_nat_cps, fw_cps across all the partitions. To view this data per partition, execute the show system app-performance command. For the Multi-PU systems, the system-wide CPU value is the sum total across the Processing Units (PUs). The number of logs or traps are limited to a maximum of one in every 3 minutes. You can specify 0-2147483647 threshold value. Default value is 0 which turns off the CPS threshold monitoring. To turn on/off the related traps, execute the snmp-server enable traps command. To view the CPS log, execute the show log command. For more information, see the examples below.
log-session-on-established	Sends TCP session creation log on completion of three-way handshake.
msl-time *seconds*	Configures the maximum session life for client sessions. You can specify 1-39 seconds. The default value is 2 seconds.
sessions-	Sets a value for the system-wide sessions

Option	Description
threshold *num*	threshold. A trap and a log is generated when the following events occur: • Number of sessions in the system exceeds the configured threshold. • Number of sessions in the system subsequently subceeds the configured threshold. For the Multi-PU systems, the system-wide value is the sum total across the Processing Units (PUs). The number of logs or traps are limited to a maximum of one in every 3 minutes. You can specify 0-2147483647 threshold value. Default value is 0 which turns off the sessions threshold monitoring. To turn on/off the related traps, refer the snmp-server enable traps CLI. To view the sessions log, execute the show log command. For more information, see the examples below.
timer-wheel-walk-limit *num*	Specifies the timer wheel walk limit. You can specify 0-1024 value, where 0 is unlimited and default value is 100.

Default The default threshold value is '0'.

Mode Global configuration mode

Example The following are the configuration examples:

```
ACOS(config)# system apps-global cps-threshold 10000
ACOS(config)# system apps-global log-session-on-established
ACOS(config)# system apps-global msl-time 10
ACOS(config)# system apps-global sessions-threshold 80000
ACOS(config)# system apps-global timer-wheel-walk-limit 500
```

The following example shows the log when CPS goes above the configured threshold:

```
ACOS(config)# show log
```

```
Log Buffer: 30000
May 11 2022 21:55:02 Info        [ACOS]:The current
Connections Per Second (CPS) 11000 in the system has gone
above the threshold 10000
```

The following example shows the log when CPS goes below the configured threshold:

```
ACOS(config)# show log
Log Buffer: 30000
May 11 2022 22:00:02 Info        [ACOS]:The current
Connections Per Second (CPS) 9500 in the system has gone above
the threshold 10000
```

The following example shows the log when number of sessions goes above the configured threshold:

```
ACOS(config)# show log
Log Buffer: 30000
May 11 2022 21:55:08 Info        [ACOS]:The current number of
sessions 810000 in the system has gone above the threshold
800000
```

The following example shows the log when number of sessions goes below the configured threshold:

```
ACOS(config)# show log
Log Buffer: 30000
May 11 2022 22:10:02 Info        [ACOS]:The current number of
sessions 790000 in the system has gone below the threshold
800000
```

Related Commands:

- snmp-server enable traps

system attack log

Description Enable logging for DDoS attacks.

Syntax

```
[no] system attack log
```

Default Disabled

Mode Configuration mode

system bandwidth

Description Display system bandwidth counters that can be enabled baselining.

Syntax

```
[no] system bandwidth [critical-threshold | sampling-enable
options | warning-threshold]
```

Option	Description
critical-threshold	Modify the default critical threshold for modular licensing bandwidth usage. The threshold range can be set from 81-99%. By default, when the bandwidth reaches 95% and sustains for two consecutive days, the critical message alert is sent to ACOS using the Syslog and SNMP trap.
warning-threshold	Modify the default critical threshold for modular licensing bandwidth usage. The threshold range can be set to 81-99%. By default, the Syslog and SNMP traps send the critical message alert to ACOS when the bandwidth reaches 95% and sustains for two consecutive days. Similarly, when the bandwidth hits 100%, ACOS receives the emergency message alert.
sampling-enable *options*	Enable baselining on system-level and view counters. The available options are: • **all** - Enable all available counters on system-level. • **input-bytes-per-sec** - Enable baselining and rate calculation for input bytes per second

Option	Description
	counter. • **output-bytes-per-sec** - Enable baselining and rate calculation for output bytes per second counter.

Mode Configuration Mode

Example The following command enables baselining and rate calculation for the input-bytes-per-sec counter.

```
ACOS(config)# system bandwidth sampling-enable input-bytes-per-sec
```

Example The following command enables warning bandwidth for modular licensing. When the threshold exceed 70% usage, the Syslog and SNMP traps will be sent.

```
ACOS(config)# system bandwidth warning-threshold 70
```

Additional Notes:

- Every hour, the system will send an alert message. However, only one of the two alerts (critical or warning) may be sent at a time. If both the threshold conditions are met, the critical alert will take priority over warning alert.
- When the bandwidth hits 100%, an emergency alert is sent.
- You cannot remove the bandwidth configurations from the system using **no system bandwidth {warning-threshold | critical-threshold}** command. Instead, the system will revert to the default threshold values 75% and 95% respectively.

For more information, see *System Administrator and Configuration Guide*.

Related Commands:

- acos-events
- snmp-server enable service
- snmp-server enable traps
- snmp-server host

system bfd

Description Display Bidirectional Forwarding Detection (BFD) statistics.

Syntax

```
[no] system bfd [sampling-enable options]
```

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
all	all packets.
ip_checksum_error	
udp_checksum_error	UDP packet checksum errors
session_not_found	
multihop_mismatch	Multihop session or packet mismatch
version_mismatch	BFD version mismatch
length_too_small	Packets too small
data_is_short	Packet data length too short
invalid_detect_mult	Invalid detect multiplier
invalid_multipoint	Invalid multipoint setting
invalid_my_disc	Invalid my descriptor
invalid_ttl	Invalid TTL
auth_length_invalid	Invalid authentication length
auth_mismatch	
auth_type_mismatch	Authentication type mismatch
auth_key_id_mismatch	Authentication key-id mismatch
auth_key_mismatch	Authentication key mismatch
auth_seqnum_invalid	Invalid authentication sequence number
auth_failed	Authentication failures
local_state_admin_down	Local admin down session state
dest_unreachable	Destination unreachable
other_error	Other errors

Mode Configuration Mode

system-big-buff-pool big-buff-pool

Description On high-end models only, you can enable the **system-big-buff-pool big-buff-pool** option to expand support from 4 million to 8 million buffers and increase the buffer index from 22 to 24 bits.

Syntax **system-big-buff-pool big-buff-pool**

Default Disabled

Mode Configuration mode

Example The following commands enable a larger I/O buffer pool for Thunder:

```
ACOS(config)# system-big-buff-pool big-buff-pool
This will modify your boot profile to disable big I/O buffer
pool.
It will take effect starting from the next reboot.
Please confirm: You want to disable the big I/O buffer pool
(N/Y)?:
Y
```

system chassis-port-split

Description Enable port splitting for the Multi-PU platforms.

NOTE: The command is applicable only to FTA-devices.

Syntax **[no] system chassis-port-split enable**

Default Disabled

Mode Global Configuration Mode

Usage The 64k ports are evenly split between PU1 and PU2. The ports 0 to 32k are for PU1, and 33k – 64K are for PU2.

NOTE: The command takes effect only if you save the configuration using the **write memory command** and then reboot using the **reboot** command.

Example

```
ACOS(config)# system chassis-port-split enable
```

Related Commands:

- odd-even-nat-enable
- vlan
- interface

system cli-session-limit

Description Configure the maximum number of concurrent CLI sessions allowed on the system (2-256).

Syntax

```
[no] system cli-session-limit num
```

Default 256

Mode Global configuration

Example Allow a maximum of 100 concurrent CLI sessions.

```
ACOS(config)# system cli-session-limit 100
```

system config-mgmt

Description Specifies the system configuration management setting for deleting referenced SLB objects.

Syntax

```
[no] system config-mgmt delete-referenced-tagged-objects [
enable | disable ]
```

Parameter	Description
delete-referenced-tagged-objects enable	Enables the deletion of SLB objects that are tagged and referenced elsewhere in the system. When this command is enabled, the system allows the deletion of SLB objects even if they are referenced by other configurations or objects within the system.

Parameter	Description
delete-referenced-tagged-objects disable	Disables the deletion of SLB objects that are tagged and referenced elsewhere in the system. When this command is disabled, the system prevents the deletion of SLB objects (virtual-server, service-group, and real server) that are referenced elsewhere in the system. If such referenced object is deleted, a message is displayed indicating the SLB object cannot be deleted because it is currently referenced by other objects. The references must be identified and removed manually.

Default Enabled

Mode Configuration mode

Example In the following example, the deletion of referenced tagged objects is disabled. An attempt is made to delete a server object named 's1', which is referenced elsewhere in the system. The system blocks the deletion and prompts the user to remove those references first.

```
ACOS(config)# system config-mgmt delete-referenced-tagged-objects disable
ACOS(config)# no slb server s1
This object has other objects referencing this. Please remove references first.
```

Related Commands:

- slb server
- slb service-group
- slb virtual-server
- slb template

system config-mgmt notification

Description Configure the notification settings for configuration management events.

Syntax `[no] system config-mgmt notification`

This command changes the CLI to the configuration level for configuration management, where the following command is available:

Parameter	Description
period *<0-60>*	Specify the interval at which Kafka notifications are sent from the ACOS device to A10 Control. You can specify a value in the range of 0 to 60 seconds. The default value is 15 seconds.

Default 15 seconds

Mode Configuration mode

NOTE: This command is available only for the shared partition but, once configured, applies system-wide to all partitions.

Example The following command sets the Kafka notification interval to 30 seconds:

```
ACOS(config)# system config-mgmt notifications
ACOS(config-notifications)# period 30
```

system config-mgmt pu-sync-detection

Description Detects the status of configuration synchronization between PU1 and PU2 in Multi-PU platforms. This command applies only to Multi-PU platforms.

Syntax `[no] system config-mgmt pu-sync-detection`

Parameter	Description
pu-sync-detection	The actions to detect configuration synchronization between PU1 and PU2.

This command allows you to enable, disable, and set the interval for configuration synchronization detection.

Command	Description
enable	Enables the detection of configuration synchronization between PU1 and PU2.
disable	Disables the detection of configuration synchronization between PU1 and PU2.
interval	Time interval in seconds to detect configuration synchronization between PU1 and PU2. You can specify 30-86400 seconds. The default is 30 seconds. **NOTE:** The shorter period is not recommended because it could potentially cause an increase in CPU usage.

Default Disabled

Mode Configuration mode

Example The following command enables the detection of configuration synchronization between PU1 and PU2:

```
ACOS(config)# system config-mgmt pu-sync-detection
ACOS(config-pu-sync-detection)# enable
```

Example The following command sets a 75 seconds interval to detect configuration synchronization between PU1 and PU2:

```
ACOS(config)# system config-mgmt pu-sync-detection
ACOS(config-pu-sync-detection)# interval 75
```

system config-version

Description Displays the versioning information for the device configuration.

Syntax `system config-version`

Parameter	Description
version *<major.minor>*	Indicates the configuration version number in the

Parameter	Description
	format *<major.minor>*, which changes automatically whenever the configuration changes. Major version is directly set by A10 Control to differentiate the base version. Minor version is updated when changes are made through the ACOS device (CLI/aXAPI).
updated-at	Indicates the timestamp of the configuration version change. The timestamp is in the format `MM-DD HH:MM:SS TZ YYYY` (month–day, time with seconds, time zone, and year). For example: `08-23 23:56:05 IST 2025`.
modified-by	Indicates the user who modified the configuration. This field displays the username of the user who made the change. The username can be: • **admin** • A user authenticated through an LDAP server, a RADIUS server, the local user management module, or other supported authentication source.

Mode Global configuration

Usage This command is used for automatic synchronization of configuration changes between Thunder devices and A10 Control. It eliminates the need for manual configuration scans, ensuring real-time consistency across platforms.

The fields of this command are non-configurable and are incremented automatically when the configuration changes. The values can be viewed using the **show running-config system** command.

NOTE: The **version** and **updated-at** parameters can be set using aXAPI.

Example The following output shows the current configuration version details. It shows the version number, the timestamp of the last version change, and the user who modified the configuration.

```
ACOS(config)# show running-config system config-version
!Section configuration: 102 bytes
!
system config-version
 version 0.22
 updated-at "09-01 17:36:27 IST 2025"
 modified-by admin
!
```

system control-cpu

Description Display system control CPU information.

Syntax

```
[no] system control-cpu
```

Mode Configuration mode

system cpu-packet-prio-support

Description Both the Thunders for Bare Metal and ESXi support the CPU packet prioritization feature. It uses the NIVIDA Mellanox Connect-X5 card hardware programmable flow rules to classify and prioritize control packets, such as BGP, LACP, and OSPF packets, over the data packets coming to the CPU.

Syntax

```
system cpu-packet-prio-support [enable | disable]
```

Mode Configuration mode

system cpu-load-sharing

Description The CPU Round Robin feature can be used to mitigate the effects of Denial of Service (DoS) attacks that target a single CPU on the ACOS device. You can use this command to configure thresholds for CPU load sharing. If a threshold is exceeded, CPU load sharing is activated, and additional CPUs are enlisted to help process traffic and relieve the burden on the targeted CPU. A round robin algorithm distributes

packets across all of the other data CPUs on the device. Load sharing will remain in effect until traffic is no longer exceeds the thresholds that originally activated the feature.

NOTE: A10 recommends disabling this option when the layer 7 virtual port is configured on the system. When CPU load sharing is triggered, the L7 virtual port traffic will potentially be dropped, causing packet loss, retransmission, and connection reset.

Syntax

```
[no] system cpu-load-sharing
{
allow-l7-sessions |
cpu-usage low percent |
cpu-usage high percent |
disable |
disallow-new-sessions tcp|
disallow-new-sessions udp|
packets-per-second min num-pkts
}
```

Parameter	Description
allow-l7-sessions	Allows Layer 7 (L7) session packets to be forwarded to the home CPU for processing during the CPU load-sharing mode.
cpu-usage low *percent*	Lower CPU utilization threshold. Once the data CPU utilization rate drops below this threshold, then CPU round robin redistribution will stop. The default is 60, but you can specify 0-100 percent.
cpu-usage high *percent*	Upper CPU utilization threshold. Once the data CPU utilization rate exceeds this threshold, then CPU round robin redistribution will begin. The default is 75, but you can specify 0-100 percent.
disable	Disables CPU load sharing. The CPU round robin feature is not used, even if a triggering threshold is breached.
disallow-new-sessions *tcp*	Disallows the creation of new TCP sessions.
disallow-	Disallows the creation of new UDP sessions.

Parameter	Description
new-ses-sions *udp*	
packets-per-second min *num-pkts*	Maximum number of packets per second any CPU can receive, before CPU load sharing is used. You can specify 0-30000000 (30 million) packets per second.

Default The CPU load sharing feature is enabled. The thresholds have the following default values:

- cpu-usage low – 60 percent
- cpu-usage high – 75 percent
- packets-per-second – 100000

Mode Configuration mode

Usage If a hacker targets the ACOS device by repeatedly flooding the device with many packets that have the same source and destination ports, this could overwhelm the CPU that is being targeted. However, the CPU load sharing feature (which is enabled by default) protects the device by using a round robin algorithm to distribute the load across multiple CPUs when such an attack is detected.

ACOS will activate this round robin distribution across multiple CPUs if all of the following conditions occur:

1. If the utilization rate of the CPU being targeted exceeds the configured high threshold (which has a default value of 75%), AND
2. If the CPU being targeted is receiving traffic at a rate that exceeds the minimum configured threshold (the default is 100,000 packets per second), AND
3. If the CPU being targeted is receiving significantly more traffic than the other CPUs on the ACOS device. If all CPUs are under a heavy load, there would be no advantage to using round robin to distribute the traffic. Therefore, the CPU being targeted must have an elevated utilization rate that is at least 50% higher than the median utilization rate of its peer CPUs. (For example, this criterion would be met if the non-targeted CPUs have a median packet flow

of 100,000 packets per second, but the targeted CPU is receiving packets at a rate exceeding 150,00 packets per second, in which case it would be 50% higher than the median of the rate of the other processors).

ACOS will de-activate CPU round robin mode and return to normal mode when the first criterion, and either 2 or 3 above are no longer true.

For example, CPU round robin mode will cease:

4. If the targeted CPU utilization rate drops below the low threshold (default is 60%), **AND**
   - If the targeted CPU is receiving packets at a rate below the minimum configured packets-per-second threshold, **OR**
   - If the utilization rate of the targeted CPU is no longer 50% higher than the median of its neighboring CPUs.

system data-cpu

Description Display system data CPU information.

Syntax `[no] system data-cpu`

Mode Configuration mode

system ddos-attack

Description Enable logging for DDoS attack events.

Syntax `[no] system ddos-attack log`

Mode Configuration mode

system dns

Description Displays DNS statistics for the packet as per the options specified. Also, the default authoritative name server for recursive DNS can be configured.

Syntax `[no] system dns [recursive-nameserver options| sampling-enable options]`

The following options are available under **system dns**:

Option	Description
recursive-nameserver	Configures the default DNS authoritative name servers for recursive DNS resolver. **Note**: **NOTE:** • Maximum of 16 IPv4 or IPv6 name servers can be configured for each L3v partition. • If customized name servers are configured, the recursive DNS resolver uses these servers as default authoritative servers to send the first query in each layer of recursive process instead of the root name servers.
Specify one of the following options for **recursive-nameserver**:	
A.B.C.D	Specify IPv4 server address.
A:B:C:D:E:F:G:H	Specify IPv6 server address.
follow-shared	This option is available only for private L3v partition. Specify this option to use the configured name server of the shared partition in the private partition. **NOTE:** The **follow-shared** option and the configurable name server cannot be enabled at the same time.
sampling-enable	Enables baselining. This command enhances the information that can be viewed for statistical counters in the sys-

Option	Description
	tem.
Specify one of the following options for **sampling-enable**:	
all	Enables sampling of all DNS event types
slb_req	Total number of requests.
slb_resp	Total number of responses.
slb_no_resp	Total number of requests with no response
slb_req_rexmit	Total number of requests that were retrans-mitted.
slb_resp_no_ match	Total number of responses with no match.
slb_no_resource	Total number of resource failures.
nat_req	Total number of NAT requests.
nat_resp	Total number of NAT responses.
nat_no_resp	Total number of NAT requests with no response.
nat_req_rexmit	Total number of NAT requests that were retransmitted.
nat_resp_no_ match	Total number of NAT responses with no match.
nat_no_resource	Total number of NAT resource failures that occurred.
nat_xid_reused	Total number of NAT requests reusing a transaction ID.
filter_type_ drop	Total number of queries dropped due to the query type filter policy.
filter_class_ drop	Total number of queries dropped due to query class filter policy.
filter_type_ any_drop	Total number of ANY-type queries dropped due to query type filter policy.
slb_dns_client_	Total number of SSL client-side sessions

Option	Description
ssl_succ	that connected successfully.
slb_dns_server_ssl_succ	Total number of SSL server-side sessions that connected successfully.
slb_dns_udp_conn	Total number of backend UDP connections.
slb_dns_udp_conn_succ	Total number of backend UDP connections that were established.
slb_dns_padding_to_server_removed	Total number of EDNS(0) padding to the server that were removed.
slb_dns_padding_to_client_added	Total number of EDNS(0) padding to client there were added (if client SSL is configured).
slb_dns_edns_subnet_to_server_removed	Total number of EDNS(0) client subnet from client queries that were removed.
slb_dns_udp_retransmit	Total number of SLB DNS UDP that were retransmitted.
slb_dns_udp_retransmit_fail	Total number of SLB DNS UDP that were retransmitted, but failed.
rpz_action_drop	Total number of actions dropped for RPZ (Response Policy Zone).
rpz_action_pass_thru	Total number of pass through actions for RPZ (Response Policy Zone).
rpz_action_tcp_only	Total number of TCP only actions for RPZ (Response Policy Zone).
rpz_action_nxdomain	Total number of NXDOMAIN actions for RPZ (Response Policy Zone).
rpz_action_nodata	Total number of NODATA actions for RPZ (Response Policy Zone).
rpz_action_	Total number of Local Data actions for RPZ

Option	Description
local_data	(Response Policy Zone).
slb_drop	Total number of DNS requests dropped.
nat_slb_drop	Total number of NAT DNS requests dropped.
invalid_q_len_to_udp	Total number of queries with invalid query length to convert to UDP.

Mode Configuration mode

Usage The **sampling-enable** command is used to enable baselining of DNS statistics.

The **recursive-nameserver** command configures the default authoritative name server for recursive DNS.

Example Example to configure follow-shared option for private partition p1:

```
vThunder (config)#active-partition p1
vThunder (config)#system dns recursive-nameserver
vThunder [p1] (config-recursive-nameserver)#follow-shared
```

system dynamic-service-dns-socket-pool

Description Enables socket pool for dynamic service DNS. Using the command, the dynamic service sends DNS lookups via different source ports to prevent hitting the rate limitation at DNS server.

Syntax

```
[no] system dynamic-service-dns-socket-pool
```

Mode Configuration mode

Usage The command is partition-based and enables DNS socket pool for a partition where the command is run. Running the command opens 512 sockets for the partition. These sockets are not freed until DNS socket pool is disabled for the partition.

Example Example to enable DNS socket pool:

```
vThunder (config)#system dynamic-service-dns-socket-pool
```

system enable-disk-encryption

Description Enables Disk Encryption on Thunder devices. This command is applicable on the following devices:

- Thunder 3745
- Thunder 3350
- Thunder 5960

NOTE: Disabling the disk encryption is not supported.

Syntax

```
system enable-disk-encryption cipher {aes | serpent | twofish}
{passphrase <passphrase_string> | passphrase-base64 <base64_
format_passphrase>}
```

The following options are available under the above command:

Option	Description
cipher	A cipher transforms plain text into encrypted data using a specific algorithm. The resulting output, known as ciphertext, is a form of the original message that is unreadable without the correct decryption method. Without the appropriate cipher, the encrypted information cannot be deciphered. The following block ciphers are supported in cipher for encryption: • aes • serpent • twofish
passphrase	A passphrase is a string of words or characters used to secure encrypted data. It serves as a key that allows authorized users to decrypt the ciphertext and access the original readable data. The following passphrase types are supported for encryption:

Option	Description
	• passphrase - plain text string used to secure encrypted data • passphrase-base64 - string that is encoded using the base64 format.

Mode Configuration mode

Usage This command converts data into ciphertext. It helps prevent unauthorized access to sensitive information stored on disks or other storage devices, as a decryption key is required to interpret the data.

Example This command enables Disk Encryption:

```
ACOS(config)#system enable-disk-encryption cipher aes
passphrase examplestring12345
ACOS(config)#system enable-disk-encryption cipher aes
passphrase-base64 ZXhhbXBsZXN0cmluZzEyMzQ1
```

In this example, the plain-text is **examplestring12345**, and base-64 encoded is **ZXhhbXBsZXN0cmluZzEyMzQ1**.

system enable-password follow-password-policy

Description Specifies that the input of enable-password must follow the configured password-policy complexity.

Prerequisite The password-policy complexity must be configured at the system level.

Syntax

```
[no] system enable-password follow-password-policy
```

Default NA

Mode Global configuration mode

Usage This command enables the password policy check for the input of the enable-password command. As per the system password-policy complexity configured, this command ensures that the input of enable-password meets the configured password-policy requirement.

Usage If the system password-policy complexity is not configured, this command does not check the input of enable-password.

Example The following example shows how the system rejects an attempt to set the enable-password 'thiisis@t8st' when the system password-policy complexity is set to Strict repeat-character-check enable as the password does not comply with the duplicate character check and Strict password policy requirements.

```
ACOS(config)#enable-password
Password:       <<input 'thiisis@t8st' is not a valid
password>>
Retype password: <<input 'thiisis@t8st'>>
Invalid password. Does not match password requirements.
```

Example The following example indicates how the system rejects enable-passwords when the system password-policy complexity is set to Default with repeat-character and consecutive-characters checks enabled. The first two passwords when set, have failed, whereas the third password 'a10$PasSword' is accepted.

```
ACOS(config)#enable-password
Password:       <<input 'AUIDUY@4512' is not a valid password
as it does not contain lower case letters>>
Retype password: <<input 'AUIDUY@4512'>>
Invalid password. Does not match password requirements.

ACOS(config)#enable-password
Password:       <<input 'a10#Password' is not a valid password
as it repeats a character>>
Retype password: <<input 'a10#Password'>>
Invalid password. Does not match password requirements.

ACOS(config)#enable-password
Password: <<input 'a10$PasSword'>>
Retype password: <<input 'a10$PasSword' is successful>>
ACOS(config)# <<Indicates that the enable-password is
successfully changed.>>
```

Related Commands:

- system password-policy complexity
- enable-password

system fips

Description Enable/Disable FIPS Compatibility Mode for non-FIPS ACOS devices.

When operating in FIPS (Federal Information Processing Standard) Compatible Mode, ACOS will support FIPS-140-2 compliant security. FIPS compliant features and capabilities are described in the "FIPS Support" chapter in the *System Configuration and Administration Guide*.

Syntax

```
[no] system fips option
```

Option	Description
enable	Enables FIPS Compatibility Mode for the device.
disable	Disables FIPS Compatibility Mode for the device.

Default Disabled.

Mode Configuration mode

Usage This command is only supported for management sessions where the CLI is being access through the console of the ACOS device.

A reboot is required to place this command into effect.

NOTE: There are some limitations to the ACOS devices on which this command is supported. Refer to the "FIPS Compatibility Mode for Non-FIPS ACOS Devices" chapter in the *System Configuration and Administration Guide* for information on the range of ACOS devices that will support this feature.

Example The following command enables FIPS support:

```
ACOS(config)# system fips enable
FIPS support will be enabled when the system comes back up
after reboot.
Please reboot the system when you are ready.
```

Example The following command disables FIPS support:

```
ACOS(config)# system fips disable
```

```
FIPS support will be disabled when the system comes back up
after reboot.
Please reboot the system when you are ready.
```

system geo-db-hitcount-enable

Description Enable the geo database hits counter.

Syntax

```
system geo-db-hitcount-enable
```

Default Disabled

Mode Global Configuration Mode

Usage Enable hit counter after loading the geo-database.

Example

```
ACOS(config)# system geo-db-hitcount-enable
```

system geo-location

Description Loads or unloads the geo-location list to the system. By default, the **iana** database is loaded.

Syntax

```
[no] system geo-location {entry name | load {name | iana |
GeoLite2-City | GeoLite2-Country}}
```

Parameter	Description
no	Unloads the specified geo-location entry or file.
entry	Manually configure geo-location entry.
<name>	Specify geo-location name of length 1 to 127 and section range (1-15).
load	Loads the specified Geo-Location Database. You can specify one of the following: • **GeoLite2-City** - Load the built-in maxmind GeoLite2-City database which is available from http://www.maxmind.com • **GeoLite2-Country** - Load the built-in maxmind

Parameter	Description
	GeoLite2-Country database which is available from http://www.maxmind.com • **iana** - Load built-in IANA database. • *name* - Specify a geo-location file to be loaded. The string length for the file name can be minimum 1 to 63 characters.

Mode Global Configuration Mode

Usage Used to load geo-location lists that are accessible ACOS system-wide.

NOTE: Geo-location databases are not fully supported on Multi-PU Platforms (such as TH7650 and TH8665). The databases do not synchronize with both PUs after being loaded.

Example The following example shows load:

```
ACOS(config)# no system geo-location load iana
ACOS(config)# system geo-location load USER_DB
ACOS(config)# system geo-location load GeoLite2_Country
```

system glid

Description Apply a combined set of IP limiting rules to the whole system.

Syntax `[no] system glid num [non-shared]`

Default None

Command	Description
num	Replace num with the global LID that you want to use.
non-shared	Applies global limit ID to the entire system at per data CPU level. This is disabled by default.

Mode Configuration mode

Usage This command uses a single global LID from shared partition. It can only be applied at shared partition.

Example The following commands configure a standalone IP limiting rule to be applied globally to all IP clients (the clients that match class list "global"):

```
ACOS(config)# glid 1
ACOS(config-glid:1)# conn-rate-limit 10000 per 1
ACOS(config-glid:1)# conn-limit 2000000
ACOS(config-glid:1)# over-limit forward logging
ACOS(config-glid:1)# exit
ACOS(config)# system glid 1 500000 per 10
```

To apply glid at per data CPU level in non-shared mode:

```
ACOS(config)#system glid 1 non-shared 10639 per 10
```

Related Commands:

- glid

system hardware-accelerate session-forwarding

Description Enable hardware offloading feature for CGN and Firewall sessions by configuring this command. Up to 128K IPv4 sessions or 64K IPv6 sessions can be offloaded to the hardware using this command.

Hardware offloading frees up the CPU cycles, thereby enhancing the overall throughput, efficiency, and latency of the Thunder device.

NOTE: This command can be used only on Thunder devices that include Security Policy Engine (SPE) hardware acceleration capabilities.

Syntax

```
[no] system hardware-accelerate session-forwarding
```

Default Disabled

Usage Only the following sessions can be offloaded to the hardware:

- CGN LSN (NAT44) and NAT64
- Fixed NAT

- Firewall (only TCP and UDP traffic)

Additionally, only active sessions can be forwarded; standby sessions cannot be forwarded.

Mode Configuration mode

Example The following command enables hardware forwarding:

```
ACOS(config)# system hardware-accelerate session-forwarding
```

system health-check

Description Configure the individual health monitor/check object and then configure the layer 2 BFD settings.

NOTE: If you have already configured the global-level **l2-bfd** settings, this will take precedence over the **system health-check** setting.

Syntax

```
[no] system health-check monitor_name {l2-bfd | rx-interval | tx-interval | multiplier}
```

Parameter	Description
monitor_name	Specify the health monitor object name.
l2-bfd	Enable the layer 2 BFD setting.
rx-interval *<48-1000>*	Specify the minimum amount of time (in milliseconds) that the ACOS device waits to receive a BFD control packet from a BFD neighbor. If a control packet is not received within the specified time, the multiplier (below) is incremented by 1. The value can be between 48-1000 milliseconds. By default, the value is set to 800.
tx-interval <48-1000>	Specify the transmit interval (in milliseconds) between BFD packets. The value can be between 48-1000 milliseconds. By default, the value is set to 800.

Parameter	Description
multiplier *<3-50>*	Specify the maximum number of consecutive times the ACOS device will wait for a BFD control packet from a neighbor. If the multiplier value is reached, the ACOS device concludes that the routing process on the neighbor is down. The value can be between 3-50. By default, the value is set to 4.

Default As mentioned in the table

Mode Global Configuration mode

Example The following command sets the layer 2 health monitoring settings for the individual health monitor object:

```
ACOS(config)# system health-check hm-test
ACOS(config-health-check)# l2-bfd rx-interval 50 tx-interval
50 multiplier 3
```

Related Commands:

- l2-bfd
- system path

system high-memory-l4-session

Description Enable system high memory L4 session.

NOTE: The command is applicable only to FTA-devices.

Syntax

```
[no] system high-memory-l4-session enable
```

Default Disabled

Mode Global Configuration Mode

Usage If this command is enabled, ACOS will support the Thunder 7650 devices to offload RAM to maximize the memory for L4 sessions.

NOTE: To apply this command, you must save the configuration using the **write memory command** and then reboot the system using the **reboot** command.

Example The following command enables the system high memory L4 session:

```
ACOS(config)# system high-memory-l4-session enable
```

Related Commands:

- system resource-usage

system icmp

Description Display ICMP statistics.

Syntax

```
[no] system glid num [sampling-enable options]
```

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
all	all
num	Total number
inmsgs	In Messages
inerrors	In Errors
indestunreachs	In Destination Unreachable
intimeexcds	In TTL Exceeds
inparmprobs	In Parameter Problem
insrcquenchs	In Source Quench Error
inredirects	In Redirects
inechos	In Echo requests
inechoreps	In Echo replies
intimestamps	In Timestamp
intimestampreps	In Timestamp Rep

Option	Description
inaddrmasks	In Address Masks
inaddrmaskreps	In Address Mask Rep
outmsgs	Out Message
outerrors	Out Errors
outdestunreachs	Out Destination Unreachable
outtimeexcds	Out TTL Exceeds
outparmprobs	Out Parameter Problem
outsrcquenchs	Out Source Quench Error
outredirects	Out Redirects
outechos	Out Echo Requests
outechoreps	Out Echo Replies
outtimestamps	Out Time Stamp
outtimestampreps	Out Time Stamp Rep
outaddrmasks	Out Address Mask
outaddrmaskreps	Out Address Mask Rep

Mode Configuration mode

system icmp-rate

Description Display ICMP rate limit statistics.

Syntax `[no] system icmp-rate [sampling-enable options]`

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
all	All packets
over_limit_drop	Over limit drops
limit_intf_drop	Interfaces rate limit drops

Option	Description
limit_vserver_drop	Virtual Server rate limit drops
limit_total_drop	Total rate limit drops
lockup_time_left	Lockup time left
curr_rate	Current rate
v6_over_limit_drop	Over limit drops (v6)
v6_limit_intf_drop	Interfaces rate limit drops (v6)
v6_limit_vserver_drop	Virtual Server rate limit drops (v6)
v6_limit_total_drop	Total rate limit drops (v6)
v6_lockup_time_left	
v6_curr_rate	Current rate (v6)

Mode Configuration mode

system icmp6

Description Display ICMv6P statistics.

Syntax

```
[no] system icmp6 [sampling-enable options]

[no] system icmp6 [sampling-enable options]
```

Option	Description
all	all
in_msg	In Messages
in_errors	In Errors
in_dest_un_reach	In Destination Unreachable
in_pkt_too_big	In Packet too big
in_time_exceeds	In TTL Exceeds
in_parm_prob	In Parameter Problem
in_echos	In Echo requests
in_echo_reply	In Echo replies

Option	Description
in_grp_mem_query	In Group member query
in_grp_mem_resp	In Group member reply
in_grp_mem_reduction	In Group member reduction
in_router_sol	In Router solicitation
in_ra	In Router advertisement
in_ns	In neighbor solicitation
in_na	In neighbor advertisement
in_redirect	In Redirects
out_msg	Out Message
out_dst_un_reach	Out Destination Unreachable
out_pkt_too_big	Out Packet too big
out_time_exceeds	Out TTL Exceed
out_param_prob	Out Parameter Problem
out_echo_req	Out Echo requests
out_echo_replies	Out Echo replies
out_rs	Out Router solicitation
out_ra	Out Router advertisement
out_ns	Out neighbor solicitation
out_na	Out neighbor advertisement
out_redirects	Out Redirects
out_mem_resp	Out Group member reply
out_mem_reductions	Out Group member reduction
err_rs	Error Router solicitation
err_ra	Error Router advertisement
err_ns	Error Neighbor solicitation
err_na	Error Neighbor advertisement
err_redirects	Error Redirects

Option	Description
err_echoes	Error Echo requests
err_echo_replies	Error Echo replies

Mode Configuration mode

system ip class-e-address-range-enable

Description Enables support for Class E IP addresses (240.0.0.0/4).

Syntax `[no] system ip class-e-address-range-enable`

Mode Configuration mode

Usage When this command is enabled, the system allows the configuration of Class E addresses on network interfaces, the advertisement of these addresses through BGP, and the installation of corresponding routes into the Routing Information Base (RIB) and Forwarding Information Base (FIB).

NOTE: For changes to take effect, the system must be reloaded after configuring or deconfiguring the command.

Example The following command enables configuring Class E addresses:

```
ACOS(config)#system ip class-e-address-range-enable
```

system ip-stats, system ip6-stats

Description Display IP-related or IPv6-related statistics

Syntax `[no] system ip-stats [sampling-enable options]`

Syntax `[no] system ip6-stats [sampling-enable options]`

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
all	All
inreceives	Incoming packets received
inhdrerrors	Incoming packet header errors
intoobigerrors	Incoming packet too big errors
innoroutes	Incoming no route packet drops
inaddrerrors	Incoming packet address errors
inunknownprotos	Incoming unknown protocol packet drops
intruncatedpkts	Incoming truncated packets
indiscards	Incoming packets discarded
indelivers	Incoming packets delivered
outforwdatagrams	Outgoing forwarded datagrams
outrequests	Outgoing packets
outdiscards	Outgoing packets discarded
outnoroutes	Outgoing no route packet drops
reasmtimeout	Reassembly timed out packet drops
reasmreqds	Incoming reassembly requests
reasmoks	Incoming reassembled packets
reasmfails	Incoming reassembly requests failed
fragoks	Outgoing packets fragmented
fragfails	Outgoing packets fragmentation failed
fragcreates	Outgoing fragmented packets
inmcastpkts	Incoming multicast packets
outmcastpkts	Outgoing multicast packets

system ip-threat-list

Description Configures an IP Threat List by binding to an existing class-list.

IP Threat List is a collection of class-lists that contains IP addresses coming from threat actors or malicious actors launching threat activities and malware distribution.

Using this command, you can select the type of IP Threat list you want to create for packet filtering.

Syntax

```
[no] system ip-threat-list
```

This command enters the IP threat list configuration mode where the following commands are available:

Parameter	Description
ipv4-dest-list	Specify this option to create an IPv4 Destination Threat List. It is a class list of IPv4 destination addresses.
ipv4-source-list	Specify this option to create an IPv4 Source Threat List. It is a class list of IPv4 source addresses.
ipv6-dest-list	Specify this option to create an IPv6 Destination Threat List. It is a class list of IPv6 destination addresses.
ipv6-source-list	Specify this option to create an IPv6 Source Threat List. It is a class list of IPv6 source addresses.
ipv4-internet-host-list	Specify this option to create an IPv4 Internet Host Threat List. It is a class list of IPv4 internet-hosts/subscriber addresses.
ipv6-internet-host-list	Specify this option to create an IPv6 Internet Host Threat List. It is a class list of IPv4 internet-hosts/subscriber addresses.

After entering any of the above threat lists, the configuration mode changes, providing the following options:

Parameter	Description
class-list *list-name* **[ip-threat-action** *tem-plate_num***]**	Bind the specified class-list to any of the above-mentioned threat lists. This list functions as a blocklist, meaning traffic to or from the IPs in the list is blocked. You can also bind the class-list to an IP Threat Action Template using the **ip-threat-action** *template_num* option.
white-list *list-name*	Bind the specified class-list only to an **ipv4-internet-host-list** or an **ipv6-internet-host-list**. This list functions as an exception list, meaning, traffic to and from the IPs mentioned in this list is permitted. This option is not provided for other threat lists.

Default NA

Mode Configuration mode

Usage The IP Threat List can be configured in the shared partition only. You can create an IP Threat List and bind the class-list to it or you can configure an **IP Threat Action Template** and then bind that template to the class-list. Creating an **IP Threat Action Template** helps to set the idle timeout and logs. However, this is optional.

Usage The IPv4 and IPv6 internet host lists can track malicious internet IPs in both the directions of the data plane. For example, these lists can check the destination IP for outbound new sessions as well as the source IP for inbound new sessions. Thus, a single internet host list can be used instead of two separate lists (destination list and source list).

NOTE: You can bind up to 4 class-lists to each type of IP Threat List.

Example The following example creates an IPv4 source threat list by binding to the class-list *my_ipv4threatlist*:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-source-list
ACOS(config-ip-threat-list-ipv4-src)# class-list my_
ipv4threatlist
```

Example The following example binds the class-list to the specified IP Threat Action Template:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-source-list
ACOS(config-ip-threat-list-ipv4-src)# class-list my_
ipv4threatlist ip-threat-action 4
```

Example The following example creates an IPv4 internet host threat list by binding to *a10-ip-threatList*. This class-list is automatically generated by the GLM server.

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-internet-host-list
ACOS(config-ip-threat-list-ipv4-src)# class-list a10-ip-
threatList
```

Example The following example creates an IPv4 internet host threat list by binding to a class-list, which is imported form the A10 Defend site. An exception list is also bound to this list

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-internet-host-list
ACOS(config-ip-threat-list-ipv4-src)# class-list myA10Defend-
List
ACOS(config-ip-threat-list-ipv4-src)# white-list myExep-List
```

NOTE: For more information on IP Threat Lists, see *Firewall Configuration Guide*.

system ipsec

Description Configures Crypto Cores for IPsec processing.

Syntax

```
[no] system ipsec {crypto-core num | crypto-mem percentage |
fpga-decrypt | packet-round-robin}
```

Parameter	Description
crypto-core *num*	Assign the number of crypto cores for processing IPsec packets.

Parameter	Description
	The value can be between 0 to 64.
crypto-mem *percentage*	Assign the percentage of crypto memory for processing IPsec packets (rounded to increments of 10). The value can be between 0 to 100.
fpga-decrypt {enable | disable}	Enable or disable the FTA decryption offload. **NOTE:** This is an operational command only and not for configuration, hence this option will not appear in the show running configuration.
packet-round-robin	Enable round robin for IPsec packets.

Default N/A

Mode Configuration mode

Usage The number of cores and memory are primarily used because the hardware cryptographic accelerators are shared with other modules, such as SSL. If only IPsec is being used, set the crypto-core to the maximum value, and crypto-mem to 100 percent.

NOTE:

- The **crypto-core** and **crypto-mem** options are not supported if the SSL module mode is set to 'QAT.' Similarly, these commands do not take effect if the SSL module mode is set to 'N5-New.' To view the SSL module mode, use show hardware command.
- If no core is allocated for IPsec, IPsec encryption/decryption is software supported. However, if no core is allocated for SSL, the SSL request fails.

Example The following is the configuration example:

```
ACOS(config)#system ipsec crypto-core 30
```

system ipv6-prefix-length

Description Configures the length of the source and the destination IPv6 prefix.

- For Dual-blade Multi-PU platforms, the IPv6 prefix determines the Processing Unit (PU) that will process a received packet.
- For Scaleout, the IPv6 prefix determines the user group for the packet, which in turn determines the active node for this packet. For more information, see the *Scaleout Configuration Guide*.

Syntax

```
[no] system ipv6-prefix-length length
```

Parameter	Description
length	Prefix length, 16-128.

Default 128

Mode Configuration

Usage The IPv6 prefix length can only be configured in the shared partition. It must be less than or equal to all configured values for the user-quota-prefix-length. If the IPv6 prefix length is greater than the user-quota-prefix-length, all packets with the same user-quota prefix will not receive the same NAT IPv4 address. For more information about user-quota-prefix-length, see the *IPv4-lto- IPv6 Transition Solutions Guide*.

Example The following is the configuration example for IPv6 prefix length in Multi-PU platforms:

```
ACOS#active-partition shared
Current active partition: shared
ACOS#config
ACOS(config)#system ipv6-prefix-length 6
```

NOTE: The IPv6 prefix length must be modified only when the system is not in use.

system log-cpu-interval

Description Log occurrences where the CPU is at a high usage for a specified duration.

Syntax

```
[no] system log-cpu-interval seconds
```

Replace *seconds* with the number of consecutive seconds that the CPU must be at a high usage level before a log event is created.

Mode Configuration mode

system memory

Description Configure system parameters.

Syntax

```
[no] system memory [sampling-enable options]
```

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
all	All
usage-percentage	Memory usage percentage

Mode Configuration mode

system module-ctrl-cpu

Description Throttle CLI and SNMP output when control CPU utilization reaches a specific threshold.

Syntax

```
[no] system module-ctrl-cpu {low | medium | high}
```

Parameter	Description
low	Throttles CLI and SNMP output when control CPU utilization reaches 10 percent. This is the most aggressive setting.
medium	Throttles CLI and SNMP output when control CPU

Parameter	Description
	utilization reaches 25 percent.
high	Throttles CLI and SNMP output when control CPU utilization reaches 45 percent. This is the least aggressive setting.

Default Not set. Throttling does not occur.

Mode Configuration mode

Usage The command takes effect only for new CLI sessions that are started after you enter the command. After entering the command, close currently open CLI sessions and start a new one.

system mon-template

Description Configure a link monitoring template.

Syntax

```
[no] system mon-template { link-block-as-down | link-down-on-restart | monitor num }
```

Parameter	Description
link-block-as-down enable	Enable this option to treat an LACP Link-block event as a link-down template. **NOTE:** The current system monitor infrastructure does not support trunk monitoring; therefore, enabling or disabling an interface that is part of a trunk is not considered an LACP event. This option is not enabled by default.
link-down-on-restart enable	Enable this option to treat all Link events as link-down templates. This option is not enabled by default.
monitor *num*	Configure a monitor template. Replace *num* with

Parameter	Description
	the identification number of the template. This can be a number between 1 to 16.

The **monitor** command enters the Monitor Template Configuration mode where the following commands are available.

Command	Description
[**no**] **action** *options*	Specifies the action to perform when a monitored event is detected. • **clear sessions**{ **all** | **sequence** *num*} {all-partitions | partition *name*} - Clear sessions • **link-disable eth** *portnum* **sequence** *num* - Specify the interfaces to be disabled • **link-enable eth** *portnum* **sequence** *num* - Specify the interfaces to be enabled
[**no**] **monitor** *options*	Specifies the events and links (Ethernet data ports) to monitor. The sequence number assigned to monitoring entries specify the order in which to check the monitored ports for the specified event type. • **link-down eth** *portnum* [**eth** *portnum* ...] **sequence** *order* - Specify the interfaces to be monitored for link-down event • **link-up eth** *portnum* [**eth** *portnum* ...] **sequence** *order* - Specify the interfaces to be monitored for link-up event
[**no**] **monitor-**	Uses the logical operator “AND” for link

Command	Description
and	monitoring. The actions are performed only if *all* of the monitored events are detected. This is selected by default.
[no] monitor-or	Uses the logical operator "OR". The actions are performed if *any* of the monitored events are detected.

Default The ports within a given monitor entry are always ANDed. If you specify more than one port (eth portnum option) in the same monitor entry, the specified event must occur on all the ports in the entry. For example, if you specify link-down eth 9 eth 11, the link must go down on ports 9 and 11, for the link-state changes to count as a monitored event.

Mode Configuration mode

Usage The logical operator applies only to monitor entries, not to action entries. For example, if the logical operator is OR, and at least one of the monitored events occurs, all the actions configured in the template are applied.

You can configure the entries in any order. In the configuration, the entries of each type are ordered based on sequence number.

Example The following commands configure monitor template 1:

```
ACOS(config)# system mon-template monitor 1
ACOS(config-monitor)# monitor-or
ACOS(config-monitor)# monitor link-down eth 5 sequence 1
ACOS(config-monitor)# monitor link-down eth 6 sequence 2
ACOS(config-monitor)# action clear sessions sequence 1
partition test
ACOS(config-monitor)# action link-disable eth 5 sequence 2
ACOS(config-monitor)# action link-disable eth 6 sequence 3
```

Example The following command demonstrates **link-block-as-down** usage:

```
ACOS(config)# system mon-template link-block-as-down enable
ACOS(config)# system mon-template monitor 2
```

Example The following command demonstrates **link-block-on-restart** usage:

```
ACOS(config)# system mon-template link-block-on-restart enable
ACOS(config)# system mon-template monitor 3
```

system ndisc-ra

Description Configure neighbor discovery and RA counters.

Syntax

```
[no] system ndisc-ra [sampling-enable options]
```

Specify sampling-enable to enable baselining. The following options are available:

Option	Description
all	All
good_recv	Good Router Solicitations (R.S.) Received
periodic_sent	Periodic Router Advertisements (R.A.) Sent
rate_limit	R.S. Rate Limited
bad_hop_limit	R.S. Bad Hop Limit
truncated	R.S. Truncated
bad_icmpv6_csum	R.S. Bad ICMPv6 Checksum
bad_icmpv6_code	R.S. Unknown ICMPv6 Code
bad_icmpv6_option	R.S. Bad ICMPv6 Option
l2_addr_and_unspec	R.S. Src Link-Layer Option and Unspecified Address
no_free_buffers	No Free Buffers to send R.A.

Mode Configuration mode

system path

Description Configure the layer 2 health monitor path object.

NOTE: Before configuring this feature, ensure to configure **system health-check**.

Syntax

```
[no] system path path-object {interface-pair {ethernet | trunk} | use  monitor_name | user-tag user_tag_name}
```

Parameter	Description
path-object	Specify the path object.
interface-pair {*ethernet* | *trunk*}	Specify the interface to which the layer 2 BFD will be applied for health monitoring. The options are: • *ethernet* <*portnum*>- Specify the two ethernet data ports. • *trunk* <*trunknum*>- Specify the two trunk interface.
use *monitor_name*	Specify the name of the health monitor that is defined under **system health-check**.
user-tag *user_tag_name*	Specify the custom user tag health monitor name and then associate it with the **system health-check** command.

Default Not configured

Mode Global Configuration mode

Usage This command can be used in the case of firewall load balance by virtual wire (as part of the SSLi solution). It provides the ability to detect the status of the IP-less device.

The following process describes the workflow of this feature:

- The endpoints in the path transmits health monitoring (also known as heartbeats) signals to one another. If several health monitor packets are not received from either endpoint, the path is deemed down.
- When this path is associated to the real server, it connects the path status to the interface real server.

- If the internal path is blocked because the firewall is down, Thunder can detect the state change and notify the interface server on the path to reflect to status.
- Once the interface server update the state, the application can choose the functional server to handle next request.
- The path object will update the associated server when its state changes.
- The real server synchronizes its state according to the received event. It also query the path's state every second to ensure its state is synchronized with the path.

Example The following command enables this feature:

```
ACOS(config)#system path hm-obj-test
ACOS(config-path)#interface-pair ethernet 1 ethernet 2
ACOS(config-path)#use hm-test
```

Related Commands:

- l2-bfd
- system health-check

system password-policy complexity

Description Configures password policy complexity with password aging, password history, minimum password length, and password checks.

Syntax

```
system password-policy complexity policy_level {aging val |
history val | min-pswd-len num | username-check
[enable|disable] | repeat-character-check [enable|disable] |
forbid-consecutive-character num}

no system password-policy
```

Parameter	Description
policy_level	Specifies the password complexity. The options are as follows: • Strict • Medium

Parameter	Description
	• Default • Simple
aging *val*	Specifies the password validity after which the password expires. The options are as follows: • Strict - Maximum Age-60 Days • Medium - Maximum Age-90 Days • Simple - Maximum Age-120 Days
history *val*	Specifies the number of unique passwords that must be used before reusing the old password. The options are as follows: • Strict - Does not allow upto 5 old passwords • Medium - Does not allow upto 4 old passwords • Simple - Does not allow upto 3 old passwords
min-pswd-len *num*	Specifies the custom password length. The value can range from 8-63. This value overrides the minimum length associated with the password-policy complexity.
username-check [enable|disable]	Enables or disables password containing username check.
repeat-character-check [enable|disable]	Enables or disables password repeat character check.
forbid-consecutive-character *num*	Enables the forbid consecutive characters check by setting the length of sequential letters or numbers on the keyboard which will not be allowed. If the length value is set to either 3, 4, or 5, the check is enabled. If this length is set to zero, the check is disabled.

Default Default password-policy complexity

Mode Configuration mode

Usage This command allows you to improve the password strength.

Example The following command shows the supported password-policy complexity:

```
ACOS(config)#system password-policy complexity ?
Strict   Strict: Min length:8, Min Lower Case:2, Min Upper
Case:2, Min Numbers:2, Min Special Character:1, CHANGE Min 8
Characters
Medium   Medium: Min length:6, Min Lower Case:2, Min Upper
Case:2, Min Numbers:1, Min Special Character:1, CHANGE Min 6
Characters
Default  Default: Min length:9, Min Lower Case:1, Min Upper
Case:1, Min Numbers:1, Min Special Character:1, CHANGE Min 1
Character
Simple   Simple: Min length:4, Min Lower Case:1, Min Upper
Case:1, Min Numbers:1, Min Special Character:0, CHANGE Min 4
Characters
```

Example The following CLI command configures a medium password-policy complexity with aging of 60 days and prohibiting previous 3 passwords:

```
ACOS(config)# system password-policy complexity Medium aging
Strict history Simple
```

Example The following CLI command enables the username check for medium complexity:

```
ACOS(config)# system password-policy complexity Medium
username-check enable
```

When this check is enabled, the password cannot contain the corresponding username with same the capitalization of letters. For example, 'pass!@admin1QW' password is invalid for 'admin' user whereas 'pass!@Admin1QW' is valid.

Example The following CLI command enables the repeat character check for simple complexity:

```
ACOS(config)# system password-policy complexity Simple repeat-character-check enable
```

When this check is enabled, the password containing consecutive repeated characters of the same letter or number with the same capitalization of letters are prohibited. For example, password containing 'aa', 'AA', '11' are invalid whereas password containing 'aA', 'Aa' are valid.

Example The following CLI command enables the forbid consecutive character check for strict complexity with five consecutive characters:

```
ACOS(config)# system password-policy complexity Strict forbid-consecutive-character 5
```

When this check is enabled, the password containing sequential row keyboard input of letters or numbers are prohibited. For example, a password containing 'asdfg' or 'gfdsa' is invalid whereas a password containing 'asdf', '1234', 'fdsa', 'ASdfg', '!@#$%', 'klzxc', 'iopas', '890qw' is valid.

Example The following CLI command disables the forbid consecutive character check for strict complexity:

```
ACOS(config)# system password-policy complexity Strict forbid-consecutive-character 0
```

system pbslb sockstress-disable

Description Disable Sockstress system attack protection.

Syntax

```
[no] system pbslb sockstress-disable
```

Default Sockstress protection is enabled by default

Mode Configuration mode

system per-vlan-limit

Description Configure the packet flooding limit per VLAN.

The limit applies to each VLAN. No individual can exceed the specified limit.

To configure a global limit for all VLANs, use system all-vlan-limit.

Syntax

```
[no] system per-vlan-limit
{bcast | ipmcast | mcast | unknown-ucast} limit
```

Parameter	Description
bcast	Configure the limit for broadcast packets.
ipmcast	Configure the limit for IP multicast packets.
mcast	Configure the limit for multicast packets.
unknown-ucast	Configure the limit for unknown unicast packets.
limit	Configure the number of packets per second (1-65535).

Default 1000 packets per second.

Mode Configuration mode

Example The following example sets the packet limit to 5000 broadcast packets per second:

```
AOCS(config)# system per-vlan-limit bcast 5000
```

Related Commands:

- system all-vlan-limit

system port-count

Description Configure the number of ports to be allocated for the Linux Kernel, Health Monitor, ALG types and the Smart NATs.

If the **system chassis-port-split** command is enabled, the allocated ports are split evenly between the Master and the Blade. The ports 0 to 32k are for the Master, and 32k – 64K are for the Blade.

NOTE: Supported for TCP and UDP traffic only.

Syntax

```
[no] system port-count
```

This command enters the port-count configuration mode where the following commands are available:

Parameter	Description
alg *<num>*	Specify the number of ports to be allocated for the Application Layer Gateway (ALG) types by entering a value in the range 1000 to 6000. The default value is 6000.
hm *<num>*	Specify the number of ports to be allocated for the Health Monitor by entering a value in the range 1024 to 4096. This port range will be used by the Health Monitor Data Plane. The default value is 1024.
kernel *<num>*	Specify the number of ports to be allocated for the Linux Kernel by entering a value in the range 1024 to 24000. This port range will be used for the traffic going to the kernel. The default value is 18000.

Default NA

Mode Global Configuration mode

Usage From the 64k port range (1024 to 65534), you can configure the number of ports to be allocated for the Linux Kernel, the Health Monitor, and the ALG types. The rest of the unallocated ports are for the Smart NATs.

The following example demonstrates **port-count** usage:

```
ACOS(config)# system port-count
ACOS(config-port-count)# kernel 18000
ACOS(config-port-count)# hm 1024
ACOS(config-port-count)# alg 6000
```

Based on the number of ports configured, the ports are allocated in the following manner:

Parameter	Start Port	Number of ports allocated	End Port
Linux Kernel	1,024	18,000	19,023
Health Monitor	19,024	1,024	20,047
Logging (reserved internally)	20,048	4,096	24,143
ALG	24,143	6,000	30,143
Smart NATs	30,144	35,390 (remaining unallocated ports)	65,534

In the above example, if the **`system chassis-port-split`** command is enabled, the ports will be split and allocated for the Master in the following manner:

Parameter	Start Port	Number of ports allocated	End Port
Kernel	1,024	9,000 (18000/2)	10,023
Health Monitor	10,024	512 (1024/2)	10,535
Logging (reserved internally)	10,536	2,048 (4096/2)	12,583
ALG types	12,584	3,000 (6000/2)	15,583
Smart NATs	15,584	17,183 (remaining unallocated ports)	32,767

Similarly, the ports will be split and allocated for the Blade in the following manner:

Parameter	Start Port	Number of ports allocated	End Port
Kernel	32,768	9,000 (18000/2)	41,767
Health Monitor	41,768	512 (1024/2)	42,279
Logging (reserved internally)	42,280	2,048 (4096/2)	44,327

Parameter	Start Port	Number of ports allocated	End Port
ALG types	44,328	3,000 (6000/2)	44,627
Smart NATs	44,628	20,906 (remaining unallocated ports)	65,534

NOTE: You must save the configuration (using the **write memory command**) and then reboot (using the **reboot** command) to place this command into effect.

system ports link-detection-interval

Description Configures system ports link detection interval.

This allows to increase or decrease the detection interval to detect the link status change (Up to Down or Down to Up).

NOTE: This command is not supported on the vThunder platforms.

Syntax

```
[no] system ports link-detection-interval
```

Default 50 milliseconds to 60 seconds

Mode Configuration mode

NOTE: Setting the ports link detection interval to a lower value might result in high control CPU usage.

system prio-queue-support

Description When enabled, the command prioritizes the control plane protocol packets such as BFDs. These control packets are filtered into a separate queue where CPU prioritizes and processes these specific queues before processing packets from the other queues.

NOTE: The feature uses NIC's capability of flow redirection support.

Syntax

```
[no] system prio-queue-support enable
```

Default Not enabled.

Mode Global Configuration mode

Example
```
ACOS(config)# system prio-queue-support enable
```

Usage After executing the command to enable the feature, one of the following conditions occur:

- If the required NIC is not available, the following message is displayed:
  `Supported NIC is not present`
- If the supported NIC is available, the system must be reloaded for the changes to take effect. If the feature is enabled, the following status is mentioned in the log file after reloading the system:
  `Priority Queue Infra - Enabled`

system promiscuous-mode

Description Enable the system to pass traffic in promiscuous mode.

This setting enables an interface to pass all received traffic directly to the CPU, instead of passing only the packets that were intended for that interface. Promiscuous mode is commonly used as a tool to help diagnose network connectivity problems.

Syntax
```
[no] system promiscuous-mode
```

Default Not enabled.

Mode Configuration mode

system q-in-q

Description Enables 802.1Q-in-Q (double tag) processing. Specifying this option, allows multiple VLAN tags to be inserted into a single Ethernet frame.

Syntax
```
[no] system q-in-q
```

This command enters the Q-in-Q Configuration mode where the following commands are available:

Parameter	Description
inner-tpid *num*	Set the Tag Protocol Identifier (TPID) of the inner VLAN tags to *num*.
outer-tpid *num*	Set the Tag Protocol Identifier (TPID) of the outer VLAN tags to *num*.
enable-all-ports	Enable 802.1Q-in-Q (double tagging) support on all the physical ports (global level).

Default Disabled

Mode Configuration mode

Example The following example sets the TPID on the inner VLAN tag to 9100 and enables 802.1Q-in-Q support on all the physical ports:

```
ACOS(config)# system q-in-q
ACOS(config-q-in-q)# inner-tpid 9100
ACOS(config-q-in-q)# enable-all-ports
```

system queuing-buffer enable

Description Enable/disable micro-burst traffic support. The command is applicable only to FTA-devices

Syntax

```
[no] system queuing-buffer enable
```

Mode Configuration mode

system radius server

Description Create a RADIUS server configuration. This option can be useful for logging client attributes, such as mobile numbers, obtained from the RADIUS server.

NOTE: The system radius server CLI command replaces the deprecated CLI commands named cgnv6 lsn radius server and fw radius server. If these deprecated commands are used in old configurations, it must be replaced with system radius server. Else, an error message is displayed.

Syntax

```
[no] system radius server
```

This command changes the CLI to the configuration level for the specified RADIUS server, where the following commands are available. The other commands are common to all CLI configuration levels.

Command	Description
[no] accounting	Configures actions for RADIUS accounting messages. The following actions can be specified: • **interim-update** – Actions for accounting Interim-Update messages. The following options are available: ◦ **ignore**– Ignore the entry. ◦ **append-entry**– Append the AVPs to the existing entry. ◦ **replace-entry** – Replace the AVPs of the existing entry. • **on** – Actions for accounting On messages. ◦ **delete-entries-using-attribute** – Delete entries matching attribute in RADIUS table. The following options are available: ◦ **msisdn** – Clear using MSISDN ◦ **imei** – Clear using IMEI ◦ **imsi** – Clear using IMSI ◦ **NAME<length:1-15>** – Clear using customized attribute. ◦ **ignore** – Ignore the request. • **start** – Actions for accounting Start messages. The following options are available: ◦ **ignore**– Ignore the entry. ◦ **append-entry**– Append the AVPs to the existing entry. ◦ **replace-entry** – Replace the AVPs of the existing

Command	Description
	entry. • **stop** – Actions for accounting Stop messages. ◦ **ignore**– Ignore the entry. ◦ **delete-entry**– Delete the entry. ◦ **delete-entry-and-sessions** – Delete the entry and data sessions associated. **NOTE:** The `delete-entry-and-sessions` command is applicable for CGN sessions only.
[**no**] **attribute** *attr-name* [[**vendor** *vendor-id*] **number** *attr-id*]	Specifies the client RADIUS attributes for the ACOS device to in response to receive RADIUS Accounting requests. The following attributes can be specified: • **charging-gw-address** *num* – Charging Gateway Address. • **sgsn-address** *num* – Serving GPRS Support Node Address. • **ggsn-address** *num* – Gateway GPRS Support Node Address. • **rat-type** *num* – Radio Access Technology type. • **user-location** ***num*** - User location. • **inside-ipv6-prefix prefix-length** *num* – Framed IPv6 address. Specify the prefix-length for the Framed IPv6 address. • **inside-ip** – Inside client's IPv4 address. • **inside-ipv6** – Inside client's IPv6 address. • **imei** – Inside client's mobile number, as International Mobile Equipment Identity (IMEI). • **imsi** – Inside client's mobile number, as

Command	Description
	International Mobile Subscriber Identity (IMSI). • **msisdn** – Inside client's mobile number, as Mobile Station International ISDN Number (MSISDN). • **custom1**, **custom2**, **custom3** – Additional attributes not covered by other options. The *vendor-id* specifies the RADIUS vendor ID and can be 1-65535. The *attr-id* specifies the RADIUS attribute ID and can be 1-255. These options, in combination, allow you to specify any attribute to be used as the client's inside IP address, or MSIDSN, or IMEI, and so on. For example, if your RADIUS server normally sends the MSIDSN attribute as attribute 31, you could use the following command to configure the ACOS device to use the same attribute value for MSIDSN: **attribute msisdn number 31**
[**no**] **disable-reply**	Configures the toggle option for RADIUS reply packet.
[**no**] **listen-port** *portnum*	Specifies the port number of the RADIUS server to listen for Accounting requests. The default value for the listen port is 1813.
[**no**] **remote**	Specifies the name of the IP list that contains the IP addresses of the RADIUS clients from which to obtain mobile numbers for traffic logging. The following options are available: **ip-list** - IP list of remote clients.
[**no**] **secret** {*name* | **encrypted**}	Specifies the password string used to authenticate RADIUS traffic.

Command	Description
[no] vrid *num*	Joins a VRRP-A failover group.

Default By default, no RADIUS servers are configured. When you use this command to configure one, the server has the defaults listed in the table above.

Mode Configuration mode

Usage You can configure ACOS to use the same mechanism for inserting the MSISDN values into HTTP request headers, that is used to insert the values into CGN log messages.

Example The following commands configure RADIUS server parameters for ACOS:

```
ACOS(config)# system radius server
ACOS(config-lsn radius)# remote ip-list RADIUS_IP_LIST
ACOS(config-lsn radius)# secret a10rad
ACOS(config-lsn radius)# listen-port 1813
ACOS(config-lsn radius)# attribute inside-ip number 8
```

system resource-accounting template

Description Create a system resource-accounting template.

Syntax

```
[no] system resource-accounting template name
```

Parameter	Description
name	Name of the resource accounting template (1-63 characters).
app-resources	Contains configuration parameters for application resources such as the number of health monitors, real servers, service groups, virtual servers, as well as a number of GSLB parameters, such as GSLB devices,

Parameter	Description
	GSLB sites, and GSLB zones.[1] At the template configuration level, set the following application resource parameters: • **cache-template-cfg** *num* - Number of cache-template limits allowed • **client-ssl-template-cfg** *num*- Number of client-ssl-template limits allowed • **conn-reuse-template-cfg** *num* - Number of conn-reuse-template limits • **fast-tcp-template-cfg** *num* - Number of fast-tcp-template limits • **fast-udp-template-cfg** *num* - Number of fast-udp-template limits allowed • **fix-template-cfg** *num* - Number of fix-template limits allowed • **http-template-cfg** *num* - Number of http-template limits allowed • **link-cost-template-cfg** *num* - Number of link-cost-template limits • **persist-cookie-template-cfg** *num* - Number of persist-cookie-template limits allowed • **persist-srcip-template-cfg** *num* - Number of persist-srcip-template limits allowed • **proxy-template-cfg** *num* - Number of proxy-template limits allowed • **server-ssl-template-cfg** *num* - Number of server-ssl-template limits allowed

[1]GSLB parameters are configurable on a per-partition basis hard-coded (and thus non-configurable) at the system level.

Parameter	Description
	• **stream-template-cfg** *num* - Number of stream-template limits allowed • **gslb-device-cfg max** *num* – Number of GSLB devices allowed • **gslb-geo-location-cfg max** *num* – Number of GSLB geo-locations allowed • **gslb-ip-list-cfg max** *num* – Number of GSLB IP lists allowed • **gslb-policy-cfg max** *num* – Number of GSLB policies allowed • **gslb-service-cfg max** *num* – Number of GSLB services allowed • **gslb-service-ip-cfg max** *num* – Number of GSLB service IPs allowed • **gslb-service-port-cfg max** *num* – Number of GSLB service-ports allowed • **gslb-site-cfg max** *num* – Number of GSLB sites allowed • **gslb-svc-group-cfg max** *num* - Number of GSLB service group allowed • **gslb-template-cfg max** *num* – Number of GSLB templates allowed • **gslb-zone-cfg max** *num* – Number of GSLB zones allowed • **health-monitor-cfg max** *num* – Number of health monitor checks a server uses • **real-port-cfg max** *num* - Number of real ports allowed. • **real-server-cfg max** *num* – Number of real servers allowed • **service-group-cfg max** *num* – Number of service groups allowed

Parameter	Description
	• **threshold** *percent* – Utilization percentage at which to issue a log message and SNMP notification • **virtual-port-cfg** - Number of virtual-port limits allowed • **virtual-server-cfg max** *num* – Number of virtual servers allowed
network-resources	Contains configuration parameters for available network resources such as static ARPs, static IPv4 routes, static IPv6 routes, MAC addresses, and static neighbors. At the template configuration level, set the following application resource parameters: • **ipv4-acl-line-cfg max** *num* – Number of lines allowed in an IPv4 ACL • **ipv6-acl-line-cfg max** *num* - Number of lines allowed in an IPv6 ACL • **object-group-cfg max** *num* - Number of object group clauses allowed • **object-group-clause-cfg max** *num* - Number of object groups allowed • **static-arp-cfg** *num* – Number of static IPv4 ARPs or IPv6 neighbors allowed • **static-ipv4-route-cfg** *num* – Number of static IPv4 routes allowed • **static-ipv6-route-cfg** *num* – Number of static IPv6 routes allowed • **static-mac-cfg** *num* – Number of static MAC addresses allowed • **static-neighbor-cfg** *num* – Number of static neighbors allowed • **threshold** *percent* – Utilization percentage at which to issue a log message and SNMP notification

Parameter	Description
system-resources	Contains configuration parameters for system resources such as limits for bandwidth, concurrent sessions, Layer 4 Connections Per Second (CPS), Layer 7 CPS, NAT CPS, SSL throughput, and SSL CPS. At the template configuration level, set the following application resource parameters: • **bw-limit-cfg max** *num* – Enter the bandwidth limit in Mbps. The maximum configurable limit is 10Tbps. Right after you indicate a bandwidth limit in Mbps, optionally, disable a watermark using a **watermark-disable** keyword. A watermark is enabled by default. This means that when the bandwidth approaches the 90% mark, existing sessions will be maintained, but any new sessions will be dropped. Indicating the **watermark-disable** keyword will turn off the watermark option and result in accepting new connections until 100% of the bandwidth in that second is utilized. • **concurrent-session-limit-cfg max** *num* – Enter the concurrent session limit. • **fwcps-limit-cfg** *num* – The maximum number of convergent firewall sessions. • **l4-session-limit-cfg max** *num* – The maximum number of Layer 4 sessions. • **l4cps-limit-cfg max** *num* – The Layer 4 CPS limit • **l7cps-limit-cfg max** *num* – The Layer 7 CPS limit • **natcps-limit-cfg max** *num* – The NAT CPS limit • **sslcps-limit-cfg max** *num* – Enter the SSL CPS limit • **ssl-throughput-limit-cfg max** *num* – Enter the

Parameter	Description
	SSL throughput limit in Mbps. The maximum configurable limit is 10Tbps. Right after you indicate a bandwidth limit in Mbps, optionally, disable a watermark using a **watermark-disable** keyword. A watermark is enabled by default. This means that when the bandwidth approaches the 90% mark, existing sessions will be maintained, but any new sessions will be dropped. Indicating the **watermark-disable** keyword will turn off the watermark option and result in accepting new connections until 100% of the bandwidth in that second is utilized. • **threshold** *percent* – Utilization percentage at which to issue a log message and SNMP notification

Mode Configuration mode

Usage All the resource are configurable on per-partition basis; they are non-configurable at the system level.

Example The following command displays how to bind under a shared-partition:

NOTE: These options are configurable at the shared-partition level for limiting resources at the L3v partition level.

```
ACOS(config)# system resource-accounting template test
ACOS(config-test)#app-resources
ACOS(config-template:test-app-resources)#virtual-port-cfg max
1
ACOS(config-template:test-app-resources)#cache-template-cfg
max 1
ACOS(config-template:test-app-resources)#client-ssl-template-
cfg max 1
ACOS(config-template:test-app-resources)# conn-reuse-template-
cfg max 1
ACOS(config-template:test-app-resources)# fast-tcp-template-
cfg max 1
ACOS(config-template:test-app-resources)# fast-udp-template-
cfg max 1
```

```
ACOS(config-template:test-app-resources)# fix-template-cfg max
1
ACOS(config-template:test-app-resources)# http-template-cfg
max 1
ACOS(config-template:test-app-resources)# link-cost-template-
cfg max 1
ACOS(config-template:test-app-resources)# persist-cookie-
template-cfg max 1
ACOS(config-template:test-app-resources)# persist-srcip-
template-cfg max 1
ACOS(config-template:test-app-resources)# server-ssl-template-
cfg max 1
ACOS(config-template:test-app-resources)# proxy-template-cfg
max 1
ACOS(config-template:test-app-resources)# stream-template-cfg
max 1
```

system resource-usage

Description Change the capacity of a system resource.

Syntax

```
[no] system resource-usage resource-type
```

Command	Description
resource-type	Specifies the resource type and the maximum allowed: • **aflex-table-entry-count** - Maximum number of configurable aFlex table entries in the system. The range is platform specific. • **auth-portal-html-file-size** *num* – Maximum file size allowed for AAM HTML files (default 20 Kbytes). • **auth-session-count** *num*- Total auth sessions in the system. • **auth-portal-image-file-size** *num* – Maximum file size allowed for AAM portal image files (default 6 Kbytes). • **authz-policy-number** – Maximum number of

Command	Description
	authorization policies allowed. • **class-list-ac-entry-count** - Maximum SNI entries allowed per ACOS Device for Aho-Corasik class-lists (when used for SSL Insight bypass). The range is platform specific. • **class-list-entry-count***num* - Maximum number of class lists that the platform will support. The minimum and maximum configurable values are platform specific. • **class-list-ipv6-addr-count** - Maximum number of IPv6 addresses allowed within each IPv6 class list. The range is platform specific. • **ipsec-sa-number** - Maximum number of IPsec SAs allowed. • **l4-session-count** *num* – Maximum number of Layer 4 sessions supported. The range is platform specific. The maximum allowed l4-session-count per system is determined by dividing the device's total session capacity by the number of Processing Units (PUs). For instance, in a two-PU or Multi-PU system, the L4 session count will be half of the maximum allowed L4 session. In case of TH8665S, the maximum allowed l4-session-count per PU is 402653184. This value is half of the maximum allowed L4 sessions for the platform 805306368. **NOTE:** The show system-resource usage command displays the cumulative L4 session count in a Multi-PU system. • **max-aflex-authz-collection-number** – Maximum

Command	Description
	number of collections supported by aFleX authorization. • **max-aflex-file-size** *num* – Maximum size of an aFleX script in Kbytes. The default maximum allowable file size is 32K. • **nat-pool-addr-count** *num* – Total number of NAT pool addresses available for configuration in the system. The range is platform specific. • **ngwaf-cache-entry** *num* – Maximum number of cache entries for NGWAF. • **radius-table-size** – Total number of configurable CGNV6 RADIUS table entries. • **ram-cache-memory-limit** ***num*** – Maximum memory used by the RAM cache. The memory range is specific to the system memory of the associated hardware. For example, if the system RAM is 32GB, the memory must be between 1536 and 6144 (inclusive). • **visibility monitored-entity-count** ***num*** – Maximum number of monitored entities for visibility. The specified number must be between 3840 and162816 (inclusive). • **jwt-cache-entry** *num*– Configures the maximum number of JWT (JSON Web Token) cache entries at the system level. The configurable range is between 102400 and 1024000, depending on platform memory and system-level cache limits.

Mode Configuration mode

Usage To place a change to **l4-session-count** into effect, a reboot is required. A reload will not place this change into effect. For changes to any of the other system resources, a reload is required but a reboot is not required.

Example The following example shows how to configure the JWT cache capacity by entering a value between 102400 and the system-supported maximum value.

```
ACOS(config)# system resource-usage jwt-cache-entry 819100
```

system rfc-ipfix-ie-spec

Description Enables or Disables using the RFC-defined IPFIX information element lengths. This supports both standard and non-standard RFC field lengths to ease the integration with the collector.

Syntax

```
system rfc-ipfix-ie-spec {enable | disable}
```

Option	Description
enable	The field length of the Information Element (IE) identifier uses the RFC-defined lengths.
disable	The field length of the Information Element (IE) identifier uses non-standard lengths.

Default Disabled

Mode Configuration mode

Usage This command switches between RFC standard field lengths and non-standard field lengths.

Example The following command switches the field length of the IPFIX IE identifier to RFC-defined length:

```
ACOS(config)# system rfc-ipfix-ie-spec enable
```

system same-src-port-ip-hash

Description Enable client IP CPU-hashing when the source and destination ports are the same.

The client IP will be utilized for hashing, ensuring that the same flow is hashed to the same CPU every time.

Syntax

```
system same-src-dst-port-ip-hash enable
```

Default Disabled

Mode Configuration mode

Usage The following key points must be considered:

- The **ip client** and **ip server** commands must be configured at the interface level for the respective traffic (IPV4 or IPv6).
- The IPv4 or IPv6 source NAT pool is not supported for hashing.

Example

```
ACOS(config)# system same-src-dst-port-ip-hash enable
```

system server-cert-cache

Description Configure the server certificate caching options.

Syntax

```
[no] system server-cert-cache {age-timeout | max-cache}
```

Parameter	Description
age-timeout	Specify the aging timeout for the server certificate status cache. (1-86400 seconds)
max-cache	Specify the maximum number of server certificate status cache. (1-2400)
clear	To clear or reset functions.
do	To run exec commands in config mode.
end	To end the configure mode.
exit	To exit from configure mode or sub mode.
no	To negate the command or set its defaults.
show	To show the running system information.
write	To write the configuration.

Mode Configuration mode

system session

Description Configure session entries for different session types.

Syntax `[no] system session [sampling-enable options]`

Mode Configuration mode

system session-reclaim-limit

Description Set limits for SMP session reclaim.

Syntax `[no] system session-reclaim-limit {nscan-limit | scan-freq}`

Parameter	Description
nscan-limit	SNP session scan limit
scan-freq	SMP session scan frequency

Mode Configuration mode

system set-rxtx-desc-size {port-index<num> [rxd-size<num> | txd-size<num>]}

Description Sets the number of Descriptor size per queue.

Syntax `[no] system set-rxtx-desc-size {port-index <num> [rxd-size <num>| txd-size <num>]}`

Parameter	Description
set-rxtx-desc-size	Sets the number of Descriptor size per queue.
port-index *<num>*	Specify the port number. The value can be 0 to 4.
rxd-size *<num>*	Sets new rx-descriptor size. The value can be 0 to 65536.
txd-size *<num>*	Sets new tx-descriptor size. The value can be 0 to 65536.

Mode Configuration mode

Usage This command is supported on Baremetal, vThunder platforms, and Thunder Appliances.

Example The following command sets the number of descriptor size per queue:

```
ACOS(config)# system set-rxtx-desc-size port-index 8 rxd-size
4096 txd-size 4096
```

system set-rxtx-queue {port-index<num> [rxq-size<num> | txq-size<num>]}

Description Sets the number of Queues per port.

Syntax

```
[no] system set-rxtx-queue {port-index <num> [rxq-size <num>|
txq-size <num>]}
```

Parameter	Description
set-rxtx-queue	Sets the number of Queues per port.
port-index *<num>*	Specify the port number. The value can be 0 to 4.
rxq-size *<num>*	Set number of new rx queues. The value can be 0 to 1024.
txd-size *<num>*	Set number of new tx queues. The value can be 0 to 1024.

Mode Configuration mode

Usage This command is supported on Bare Metal, cThunder, vThunder platforms, and Thunder Appliances.

Example The following command sets the number of descriptor size per queue:

```
ACOS(config)# system set-rxtx-queue port-index 3 rxq-size 24
txq-size 24
```

system set-tcp-syn-per-sec

Description Configures the number of TCP syn packets per second. The value can be 25 to 6000.

Syntax

```
system set-tcp-syn-per-sec
```

Default 70

Mode Configuration mode

Usage This is a system-wide command to rate limit the number of TCP syn packets that are sent to the local Linux.

Example The following example configures 80 TCP syn packets per second to reach the Linux.

```
ACOS(config)# system set-tcp-syn-per-sec 80
```

system shared-poll-mode

Description Controls shared poll mode implementation.

Syntax

```
system shared-poll-mode {enable | disable}
```

Parameter	Description
enable	enable shared poll mode
disable	disable shared poll mode

Default The default value is based on the following conditions:

- For systems with 4 or more CPUs, the option is disabled by default and can be enabled if needed.
- For systems with less than 4 CPUs, the option is enabled and cannot be disabled.

Mode Configuration mode

Usage When shared poll mode is enabled, IO and data processing are performed on all cores except the control core.

This option is supported on baremetal platform and vthunders deployed on KVM, VMware, Hyperv, Azure, AWS, and Openstack.

system spe-profile

Description Creates a security policy engine profile.

Syntax

```
[no] system spe-profile {ipv4-only | ipv6-only |ipv4-ipv6}
```

Parameter	Description
ipv4-only	Enable IPv4 hardware forward entries only.
ipv6-only	Enable IPv6 hardware forward entries only.
ipv4-ipv6	Enable IPv4 and IPv6 hardware forward entries.

NOTE: The command is applicable only to FTA-devices.

system ssl-set-compatible-cipher

Description To enable or disable A10 cipher suite setting for SSL connections in the control plane.

Syntax

```
[no] system ssl-set-compatible-cipher {disable}
```

Default Enabled.

Mode Configuration mode

Example The following example disable this command.

```
ACOS(config)# system ssl-set-compatible-cipher disable
```

system ssl-req-q

Description To enable system SSL request queues statistics.

Syntax

```
[no] system ssl-req-q
```

Default Not enabled.

Mode Configuration mode

Example The following example enables this command.

```
ACOS(config)# system ssl-req-q
```

system ssl-req-q sampling-enable

Description To enable sample baselining reporting for SSL request queues.

Syntax

```
[no] system ssl-req-q sampling-enable {all | num-ssl-queues |
ssl-req-q-depth-tot | ssl-req-q-inuse-tot | ssl-hw-q-depth-tot
| ssl-hw-q-inuse-tot}
```

Parameter	Description
all	Enable sample baselineing for all the entities.
num-ssl-queues	The number of SSL request queues.
ssl-req-q-depth-tot	The total SSL request queue depth.
ssl-req-q-inuse-tot	The total SSL request queues in use.
ssl-hw-q-depth-tot	The total hardware-accelerator SSL request queues depth.
ssl-hw-q-inuse-tot	The total hardware-accelerator SSL request queues in use.

Default Not enabled.

Mode Configuration mode

Example The following example enables the sampling baseline.

```
ACOS(config)# system ssl-req-q sampling-enable ssl-req-q-
depth-tot
ACOS(config)# system ssl-req-q sampling-enable ssl-req-q-
inuse-tot
```

system ssl-scv

Description To enable or disable SSL connection server certificate validation.

Syntax

```
[no] system ssl-scv {enable}
```

Default Not enabled.

Mode Configuration mode

Example The following example enables this command:

```
ACOS(config)# system ssl-scv enable
```

system ssl-scv-verify-crl-sign

Description To enable or disable CRL signature verification during server certificate validation.

Syntax

```
[no] system ssl-scv-verify-crl-sign {enable}
```

Default Not enabled.

Mode Configuration mode

Example The following example enables this command.

```
ACOS(config)# system ssl-scv-verify-crl-sign enable
```

system ssl-scv-verify-host

Description To enable or disable checking claimed identity in the server certificate during server certificate validation.

Syntax

```
[no] system ssl-scv-verify-host {disable}
```

Default Enabled.

Mode Configuration mode

Example The following example disable this command.

```
ACOS(config)# system ssl-scv-verify-host disable
```

system table-integrity

Description Enables/ disables the table integrity checks and auto-sync options for the ARP, ND6, IPv4 FIB, IPv6 FIB, and MAC tables.
The `no system table-integrity` returns integrity checks to the default value (enable integrity and enable auto-sync).

NOTE: The command is applicable only to FTA-devices.

Syntax

```
system table-integrity all audit [enable | disable] auto-sync
[enable | disable]
```

Parameter	Description
audit enable auto-sync disable	Enables the integrity check and disables the auto-sync.
audit disable	Disables the integrity check.

Default audit and auto-sync are enabled

Mode Configuration mode

system table-integrity-check

Description Enables table integrity checks for the ARP,ND6, IPv4 FIB, IPv6, and MAC tables. An error log is generated on a per-table basis when a discrepancy is detected between the Master and Blade's table.

Syntax `[no] system table-integrity-check [enable]`

Default Disabled

Mode Configuration mode

NOTE: The command is applicable only to FTA-devices.

system tcp

Description Configure TCP counters.

Syntax `[no] system tcp [sampling-enable options]`

Specify sampling-enable to enable baselining. The following options are available:

Parameter	Description
activeopens	Active open conns
passiveopens	Passive open conns
attemptfails	
estabresets	Resets rcvd on EST conn

Parameter	Description
insegs	Total in TCP packets
outsegs	Total out TCP packets
retranssegs	Retransmited packets
inerrs	Input errors
outrsts	Reset Sent
sock_alloc	Sockets allocated
orphan_count	Orphan sockets
mem_alloc	Memory alloc
recv_mem	Total rx buffer
send_mem	Total tx buffer
currestab	Currently EST conns
currsyssnt	TCP in SYN-SNT state
currsynrcv	TCP in SYN-RCV state
currfinw1	TCP in FIN-W1 state
currfinw2	TCP FIN-W2 state
currtimew	TCP TimeW state
currclose	TCP in Close state
currclsw	TCP in CloseW state
currlack	TCP in LastACK state
currlstn	TCP in Listen state
currclsg	TCP in Closing state
pawsactiverejected	TCP paw active rej
syn_rcv_rstack	Rcv RST|ACK on SYN
syn_rcv_rst	Rcv RST on SYN
syn_rcv_ack	Rcv ACK on SYN
ax_rexmit_syn	TCP rexmit SYN
tcpabortontimeout	TCP abort on timeout

Parameter	Description
noroute	TCPIP out noroute
exceedmss	MSS exceeded pkt dropped

Mode Configuration mode

system tcp rate-limit-reset-unknown-conn {pkt-rate<num>[log]}

Description To configure rate limit for `tcp reset-on-error` command.

Syntax `system tcp rate-limit-reset-unknown-conn {pkt-rate<num>[log]}`

Parameter	Description
rate-limit-reset-unknown-conn	Configure rate limit for tcp reset-on-error.
pkt-rate	Packet rate.
num	Maximum rate to send out RESET per second (1-1048575).
log	Log when rate exceed.

Mode Configuration mode

Example The following example configures a rate limit of 11 TCP reset packets per second:

```
ACOS(config)#system tcp rate-limit-reset-unknown-conn pkt-rate
11 log
```

NOTE: The System TCP Rate Limit Resets Unknown Sessions is supported only on CGN L3V partitions for CGNv6 or FW tcp reset-on-error configuration.

system tcp-stats

Description Display TCP statistics.

Syntax `[no] system tcp-stats [sampling-enable options]`

Mode Configuration mode

system template policy

Description Globally apply a policy template to the ACOS device.

Syntax

```
[no] system template policy template-name
```

Parameter	Description
template-name	Name of the policy template (1-127 characters).

Default N/A

Mode Configuration mode

Example The following example shows the configuration of an SLB policy template "POL_TEMP" which is then applied globally using the `slb template policy` command:

```
ACOS(config)# class-list CLIST1
ACOS(config-class list)# 1.1.1.1/24
ACOS(config-class list)# 2.2.2.2/24
ACOS(config-class list)# exit
ACOS(config)# slb template policy POL_TEMP
ACOS(config-policy)# class-list CLIST1
ACOS(config-policy)# exit
ACOS(config)# system template policy POL_TEMP
```

system template-bind monitor

Description Globally apply a link monitoring template to the ACOS device.

Syntax

```
[no] system template-bind monitor template-ID
```

Parameter	Description
template-ID	ID of the monitor template (1-16).

Default N/A

Mode Configuration mode

Example This example displays the configuration of system link monitor template "1" and applies it globally using the `template-bind monitor` command:

```
ACOS(config)# system mon-template monitor 1
ACOS(config-monitor)# action link-disable eth 1 sequence 1
ACOS(config-monitor)# monitor-or
ACOS(config-monitor)# monitor link-down eth 5 sequence 1
ACOS(config-monitor)# monitor link-down eth 6 sequence 2
ACOS(config-monitor)# exit
ACOS(config)# system template-bind monitor 1
```

Example This example displays the configuration of an SLB monitor template "2" which is then applied globally using the `slb template-bind monitor` command:

```
ACOS(config)# slb template monitor 2
ACOS(config-monitor)# action link-disable eth 1 sequence 1
ACOS(config-monitor)# monitor-or
ACOS(config-monitor)# monitor link-down eth 5 sequence 1
ACOS(config-monitor)# monitor link-down eth 6 sequence 2
ACOS(config-monitor)# exit
ACOS(config)# system template-bind monitor 2
```

system timeout-value

Description Sets the timeout to stop transferring a file.

Syntax

```
[no] system timeout-value {ftp | http | https | scp | sftp | tftp} limit
```

Parameter	Description
ftp	Set timeout to stop ftp transfer in seconds, 0 is no limit (0 - 9999). Default timeout value is 120 seconds.
http	Set timeout to stop http transfer in seconds, 0 is no limit (0 - 9999).
https	Set timeout to stop https transfer in seconds, 0 is no limit (0 - 9999).

Parameter	Description
scp	Set timeout to stop scp transfer in seconds, 0 is no limit (0 - 9999). Default timeout value is 300 seconds.
sftp	Set timeout to stop sftp transfer in seconds, 0 is no limit (0 - 9999).
tftp	Set timeout to stop tftp transfer in seconds, 0 is no limit (0 - 9999).

system tls-1-3-mgmt

Description Enable or disable TLS 1.3 support on the ACOS management interface.

NOTE: TLS 1.3 will be enabled only when the ACOS comes back up after reboot or reload.

Syntax

```
[no] system tls-1-3-mgmt enable
```

Default Disabled

Mode Configuration mode

Example To enable the TLS 1.3:

```
ACOS(config)# system tls-1-3-mgmt enable
```

Example To disable the TLS 1.3:

```
ACOS(config)# no system tls-1-3-mgmt enable
```

system trunk load-balance

Description Configure trunk load balancing for Layer 2 switched packets (applicable for both static and LACP trunks).

Syntax

```
[no] system trunk load-balance
```

This command changes the CLI configuration level, where the following relevant command is available:

```
[no] layer-2 {use-l3 | use-l4}
```

Parameter	Description
use-l3	Perform load balancing based on Layer 3 (IPv4 or IPv6) parameters.
use-l4	Perform load balancing based on Layer 4 (TCP or UDP) parameters.

Default Trunk load balancing is performed based on Layer 2 (MAC) parameters.

Mode Global configuration

Usage This command is only available from the shared partition, and is applicable to all trunks configured on the system, not individual trunks.

- If the packet to be forwarded is a Layer 2 packet, Layer 2 load balancing will be used, even if `use-l3` or `use-l4` is configured.
- If the packet to be forwarded is a Layer 3 packet, a fragment, or not a TCP or UDP packet, Layer 3 load balancing will be used, even if `use-l4` is configured.

Example Configure trunk on the system to use Layer 3 load balancing:

```
ACOS(config)# system trunk load-balance
ACOS(config-load-balance)# use-l3
```

system udp skip-checksum-when-zero

Description Forwards IPv4 UDP data packets having zero checksum without recalculating the checksum.

Syntax

```
[no] system udp skip-checksum-when-zero
```

Default Disabled

Mode Global configuration

Usage When configured, this command can be applied for any ADC, CGN, and Firewall setup, including scenarios with high-speed networks that use UDP protocol such as CGN LSN NAT, or deployments like DS-Lite configurations that use UDP for tunnel encapsulation. In these cases, zero UDP checksum is enabled for high performance requirements. (See RFC 8085).

This command is only applicable for the shared partition and takes effect on the entire system including shared and network partition.

Example The following command skips the zero checksum and directly forwards the IPv4 UDP packets:

```
ACOS(config)# system udp skip-checksum-when-zero
```

system update-passphrase

Description Updates the global key that is used for configuration encryption.

Syntax

```
system update-passphrase
```

Mode Configuration mode

Usage This command is used to secure sensitive data, such as passwords. If the passphrase is lost, it cannot be recovered, and a system reset is required to downgrade the system.

Example The following command sets the new passphrase for the system:

```
ACOS(config)# system update-passphrase
Note: After changing to a new passphrase, you cannot downgrade
to the previous release. Do you want to continue with updating
to the new passphrase? [yes/no]: yes
Please enter your new passphrase (minimum 8 characters):
passwords
System passphrase update successfully.
Building configuration…
Write configuration to the default primary startup-config
```

system ve-mac-scheme

Description Configure MAC address assignment for Virtual Ethernet (VE) interfaces.

Syntax

```
[no] system ve-mac-scheme {round-robin | system-mac | hash-based}
```

Parameter	Description
round-	In the shared partition, this option assigns MAC

Parameter	Description
robin	addresses in round-robin fashion, beginning with the address for port 1. Each new VE, regardless of the VE number, is assigned the MAC address of the next Ethernet data port. For example: • The MAC address of Ethernet data port 1 is assigned to the first VE you configure. • The MAC address of Ethernet data port 2 is assigned to the second VE you configure. • The MAC address of Ethernet data port 3 is assigned to the third VE you configure. This process continues until the MAC address of the highest-numbered Ethernet data port on the ACOS device is assigned to a VE. After the last Ethernet data port's MAC address is assigned to a VE, MAC assignment begins again with Ethernet data port 1. The number of physical Ethernet data ports on the ACOS device differs depending on the ACOS model. This option is not supported in L3V partitions.
system-mac	In the shared partition, this option assigns the system MAC address (the MAC address of Ethernet data port 1) to all VEs. In an L3V partition, this option allocates a system MAC for the partition and assigns the system MAC address of the partition to all VLANs and VEs in the partition. This is useful when configuring cross connect between partitions.
hash-based	In the shared partition, this option causes ACOS to use a hash value based on the VE number to select an Ethernet data port, and assigns that data port's MAC address to the VE. This method always assigns the same Ethernet data port's MAC address to a given VE

Parameter	Description
	number, on any model, regardless of the order in which VEs are configured. This option is not supported in L3V partitions.

Default hash-based

Mode Configuration mode

Usage This command can be configured only in the shared partition, not in L3V partitions. A **reload** or **reboot** is required to place the change into effect.

Example Below is an example of the **system-mac** parameter and how it is used with L3V partitions.

First, assume we have partitions “p1” and “P2” on the device, then execute the command:

```
ACOS(config)# system ve-mac-scheme system-mac
```

After rebooting or reloading the device, examine the MAC addresses to see the mac-scheme applied on the VEs.

First, in partition “p1”:

```
ACOS[p1](config)# show interfaces brief | sec ve600
ve600 Down   N/A    N/A    N/A    600   021f.a008.01f7   0.0.0.0/0
           0
ACOS[p1](config)#
```

Next, in partition “p2”:

```
ACOS[p2]# show interfaces brief | sec ve800
ve800 Down   N/A    N/A    N/A    800   021f.a008.02f7   0.0.0.0/0
           0
ACOS[p2]#
```

Finally, in the shared partition:

```
ACOS(config)# show interfaces brief | sec ve
```

```
ve500 Down  N/A   N/A   N/A   500  021f.a008.00f7
51.51.51.2/24          1
ACOS(config)#
```

The MAC address for each partition is unique to the partition.

system-jumbo-global enable-jumbo

Description Globally enable jumbo frame support. A jumbo frame is an Ethernet frame that is more than 1522 bytes long.

This is the only command required to enable jumbo support on FTA models.

NOTE: Jumbo frames are not supported on all platforms. For detailed information, refer to the *Release Notes*.

Syntax

```
[no] system-jumbo-global enable-jumbo
```

Default Disabled

Mode Configuration mode

Usage Notes about the usage of this command:

- If your configuration uses VEs, you must enable jumbo on the individual Ethernet ports first, then enable it on the VEs that use the ports. If the VE uses more than port, the MTU on the VE should be the same or smaller than the MTU on each port.
- Enabling jumbo support does not automatically change the MTU on any interfaces. You must explicitly increase the MTU on those interfaces you plan to use for jumbo packets.
- Jumbo support is not recommended on 10/100 Mbps ports.
- On FTA models only, for any incoming jumbo frame, if the outgoing MTU is less than the incoming frame size, the ACOS device fragments the frame into 1500-byte fragments, regardless of the MTU set on the outbound interface. If it is less than 1500 bytes, it will be fragmented into the configured MTU.

- Setting the MTU on an interface indirectly sets the frame size of incoming packets to the same value. (This is the maximum receive unit [MRU]).
- In previous releases, the default MTU is 1500 and can not be set to a higher value.

NOTE: On non-FTA models, after you enable (or disable) jumbo frame support, you must save the configuration (**`write memory`** command) and reboot (**`reboot`** command) to place the change into effect.

If jumbo support is enabled on a non-FTA model and you erase the startup-config, the device is rebooted after the configuration is erased.

system-reset

Description Restore the ACOS device to its factory default settings.

Syntax

```
system-reset
```

The following table summarizes that is removed or preserved on the system:

What is Erased	What is Preserved
Saved configuration files	Running configuration
System files, such as SSL certificates and keys, aFleX policies, black/white lists, and system logs	Audit log entries
Management IP address	
Admin-configured admins	
Enable password	
Imported files	
Inactive partitions	
Enable-password follow-password-policy	

Default N/A

Mode Configuration mode

Usage This command is helpful when you need to redeploy an ACOS device in a new environment or at a new customer site, or you need to start over the configuration at the same site.

The command does not automatically reboot or power down the device. The device continues to operate using the running-config and any other system files in memory, until you reboot or power down the device.

Reboot the ACOS device to erase the running-config and place the system reset into effect.

A Default password-policy complexity is enforced when you log in for the first time after a reboot. Change the default admin password as per the default password policy complexity criteria. For more information, see *Management Access and Security Guide*.

Example The following commands reset an ACOS device to its factory default configuration, then reboot the device to erase the running-config:

```
ACOS(config)# system-reset
ACOS(config)# end
ACOS# reboot
```

Related Commands:

- erase

system-reset preserve-license

Description Restores the ACOS device license when the device is reset to its factory default settings. This is applicable only for the ACOS devices that use modular licensing.

Syntax

```
system-reset preserve-license
```

The following table summarizes what is removed and preserved on the system:

What is Erased	What is Preserved
Saved configuration files	ACOS device License
System files, including SSL certificates and keys, aFleX policies, black/white lists, and system logs	
Management IP address	
Admin-configured admins	
Enable password	
Imported files	
Inactive partitions	
Enable-password follow-password-policy	
Audit log entries	
Running configuration	

Default N/A

Mode Configuration mode

Usage This command is helpful when you want to redeploy an ACOS device in a new environment or at a new customer site, or you need to start over the configuration at the same site.

Example The following command restores the device license when an ACOS device is reset to its factory default settings:

```
ACOS(config)# system-reset preserve-license
```

Related Commands:

- system-reset
- erase

template

Description Specify or define the templates, name, list.

Syntax

```
template {csv <name> | gtp <options> | gtp-policy <name> | ip-threat-action | lid <lid_number> | limit-policy <num> | sctp {default | <name> } | syslog-over-tls }
```

Parameter	Description
csv *<name>*	Specifies CSV template name. Specify the template name (1-63 characters).
gtp *<options>*	Defines a GTP template. Replace *<options>* with the following options: • **apn-imsi-list** *<name>* **{permit|deny}** – Configures GTP APN IMSI list. • **filtering-policy** *<name>* – Configures GTP Filtering Policy. • **general-policy** *<name>* – Configures GTP General Policy. • **logging-policy** *<name>* – Configures GTP Logging Policy. • **message-filtering-policy** *<name>* **interface-type {roaming | non-roaming}** – Configures GTP Message Filtering Policy. • **msisdn-list** *<name>* **{permit|deny}** – Configures GTP MSISDN list. • **rate-limit-policy** *<name>* **{monitor | drop}** – Configures GTP Rate Limit policy. • **validation-policy** *<name>* – Configures GTP Validation Policy. Specify the name (1-63 characters).
gtp-policy <name>	Configures GTP policy name. Specify the policy name (1-63 characters).
ip-threat-action	Create an IP Threat Action Template. This template helps to enable logging and setting the idle timeout for IP threat lists.
limit-	Creates a Limit policy. Specify the limit policy number

Parameter	Description
policy *<num>*	(1 to 1023).
sctp {default | <name> }	Defines a SCTP template. Specify the template name (1-63 characters).
syslog-over-tls	Defines a syslog over TLS template.

Default NA

Mode Global Configuration mode

Usage To define different templates or license IDs.

Example Define CSV template.

```
ACOS (config)# template csv
  field 1 ip-from
  field 2 ip-to-mask
  field 3 continent
  field 4 country
  field 5 state
  field 6 city
```

template ip-threat-action

Description Create an IP Threat Action Template. This template helps to enable logging and setting the idle timeout for IP threat lists. For more information, see *Firewall Configuration* guide .

Syntax **template ip-threat-action** *template_num*

Parameters	Description
template_num	The template number. You can specify a value from 1 to 8.

This command enters the IP Threat Action Template configuration mode where the following commands are available other than the common commands:

Parameters	Description
idle-timeout *num*	Configure the idle timeout in minutes. You can specify a value from 1 to 1440. The default value is 5 minutes.
log { enable | disable }	Enable or disable logging. Logging is disabled by default.

Default NA

Mode Configuration mode

Usage Configure an IP Threat Action Template and then bind that template to the class-list.

NOTE: You can configure a maximum of 8 IP Threat Action Templates.

Example The following example demonstrates **template ip-threat-action** usage:

```
ACOS(config)# template ip-threat-action 3
ACOS(config-ip-threat-action)# idle-timeout 25
ACOS(config-ip-threat-action)# log enable
```

tacacs-server host

Description Configure TACACS+ for authorization and accounting. If authorization or accounting is specified, the ACOS device will attempt to use the TACACS+ servers in the order they are configured. If one server fails to respond, the next server will be used.

Syntax

```
[no] tacacs-server host {hostname | ipaddr}
secret secret-string [port portnum] [timeout seconds] [source
options] [prefer-data-interface] [over-tls options]
```

Parameter	Description
hostname	Host name of the TACACS+ server. If a host name is used, make sure a DNS server has been configured.
ipaddr	IP address of the TACAS+ server.
secret *secret-string*	Password, 1-128 characters, required by the TACACS+ server for authentication requests.
port *portnum*	The port used for setting up a connection with a TACACS+ server. The default port is 49.
timeout *seconds*	The maximum number of seconds allowed for setting up a connection with a TACACS+ server. You can specify a value in the range of 1 to 60 seconds. The default timeout is 12 seconds.
source	The following options are available as the source secret properties: • ethernet - The source Ethernet interface ID port number • ip - The source IPv4 address string • ipv6 - The source IPv6 address string • lif - The source logical interface ID number • loopback - The source loopback interface ID port number. • trunk - the source trunk interface ID number • ve - the source Virtual Ethernet interface ID number

Parameter	Description
`prefer-data-interface`	Specify this option to send TACACS requests along an optimal path, with preference to the data plane. When this option is set, TACACS requests are sent through the Data interface if the server is reachable through the Data plane. If the Data plane is unavailable, ACOS falls back to the Management interface for sending requests. This ensures uninterrupted and reliable TACACS communication across network environments. **NOTE:** This option is only supported when the **`source`** is set to a **`loopback`** IP address.
`over-tls`	Enables TACACS+ over TLS authentication for secure communication with Cisco Identity Services Engine (ISE). The following additional options are available for TACACS+ authentication over TLS configuration: • `cert name`[`private-key` *key*] : Specifies the client certificate and its corresponding private key for TACACS+ over TLS authentication. • `custom-ca` : Specifies the Certificate Authority (CA) certificate that ACOS uses to validate the Cisco ISE server certificate during TACACS+ over TLS

Parameter	Description
	authentication. • `skip-cert-verification`:Disables validation of the server's CA certificate during TACACS+ over TLS authentication. When this option is enabled, ACOS does not verify the authenticity of the Cisco ISE server certificate, but continues to use the configured client certificate and private key to authenticate to the server. **NOTE:** A server instance can support either "TACACS+" or "TACACS+ over TLS" authentication, but not both. These modes are mutually exclusive.

Default See descriptions.

Mode Configuration mode

Usage You can configure up to 2 TACACS+ servers. The servers are used in the order in which you add them to the configuration. Thus, the first server you add is the primary server. The second server you add is the secondary (backup) server. Enter a separate command for each of the servers. The secondary server is used only if the primary server does not respond.

Example The following command adds a TACACS+ server "192.168.3.45" and sets its shared secret as "SharedSecret":

```
[[[Undefined variable tps-sagTOC.Prompt]]](config)#tacacs-server host 192.168.3.45 secret SharedSecret
```

Example The following command adds a TACACS+ server "192.168.3.72", sets the shared secret as "NewSecret", sets the port number as 1980, and sets the connection timeout value as 6 seconds:

```
[[[Undefined variable tps-sagTOC.Prompt]]](config)#tacacs-server host 192.168.3.72 secret NewSecret port 1980 timeout 6
```

Example The following command deletes TACACS+ server “192.168.3.45:

```
[[[Undefined variable tps-sagTOC.Prompt]]](config)#no tacacs-server host 192.168.3.45
```

Example The following command deletes all TACACS+ servers:

```
[[[Undefined variable tps-sagTOC.Prompt]]](config)#no tacacs-server
```

Example The following command configures a TACACS+ server, sets the source IP to loopback interface 0, and enables the use of the data interface for sending TACACS requests:

```
ACOS(config)# tacacs-server host 10.65.16.105 secret encrypted 4L/R7ql3fq7iXNlFWhZxhxbJujg7/8VBQxOjJ2ABUgBaKVou6QizCT0Hcu9rjsjo source loopback 0 prefer-data-interface
```

Example The following command configures a TACACS+ over TLS authentication with CA verification:

```
ACOS(config)#tacacs-server host 10.19.4.210 secret 1 port 6049 over-tls cert TH_test private-key TH_test custom-ca  X_CA
```

Example The following command configures a TACACS+ over TLS authentication without CA verification:

```
ACOS(config)# tacacs-server host 10.19.4.210 secret 1 port 6049 over-tls cert TH_test private-key TH_test skip-cert-verification
```

tacacs-server monitor

Description Check the status of TACACS+ servers.

Syntax `[no] tacacs-server monitor [interval seconds]`

Parameter	Description
seconds	Frequency (in seconds) that you want the ACOS device to check the status of the TACACS+ server. You can specify 1 - 120 seconds.

Default Status checking of the TACACS+ server is not enabled. When enabled, the default interval is 60 seconds.

Mode Global configuration

Usage When TACACS+ server monitoring is configured, the ACOS device sends a TACACS+ monitor request, which contains the user name and password to the server in order to log into the device and check if the server is available. If it is, then the *last_available_timestamp* will be updated with current time.

- If a user login authentication request arrives at the ACOS device, then ACOS will send the request to the TACACS+ server that has the most recent *last_available_timestamp* value.
  - If the user's login attempt is successful, then timestamp for that server will be updated to the current time.
  - However, if the user authentication request fails, then ACOS will send the request to the secondary TACACS+ server.
- To enable this feature, you must configure the user name and password for the TACACS+ server's administrative account. While a simple server port "ping" could be used to check the status, this is not recommended because it could cause the ACOS device to be mistakenly seen as an attacker, thus causing it to be added to the ACL.

techreport

Description Configure the various parameters for show techsupport output command or log file collection. This log file is an automated collection of system information for troubleshooting and diagnosing system issues.

If you need to contact Technical Support, they might ask you to share these techreports for further investigation.

Syntax

```
[no] techreport
{disable |
enable-full-history |
hang-recover-time minutes |
interval minutes |
max-logfile-size mbytes |
max-partitions num |
priority-partition name}
```

Parameter	Description
disable	Disable the automated collection of system information.
enable-full-history	Set the retention period for the techsupport log file to 31 days (a month). This command is visible for non-FTA platform. (Only works for platform with 32GB disk size where the techreport retention period is set to 7 by default).
hang-recover-time *minutes*	Specify the device recovery time (in minutes) if the show techsupport command hangs. You can specify 15-1000 minutes.
interval *minutes*	Specify the time interval (in minutes) for collecting new data. You can specify 15-120 minutes. The default interval is 15 minutes.
max-log-file-size *gb*	Specify the maximum size (in gigabyte) of each techsupport log file that is saved on a regular basis (for a given day in a single file). You can specify 1-10 GB. The default size is 1 GB.
max-partitions *num*	Specify the maximum partitions to be displayed in each techsupport log file. You can specify 1-120. The default value is 30.
priority-partition *name*	Specify the name of the partition that should always be displayed in the techsupport log file. By default, the shared partition names are displayed.

Default Enabled.

Mode Configuration mode

Usage The techreports are a light version of the output generated or exported by theshow techsupport command.

The ACOS device saves all techreport information for a given day in a single file. The reports for each day are saved in a separate file. Timestamps indicate when each set of information was collected.

If the ACOS device is a member of an aVCS virtual chassis platform, use the **device-context** command to specify which device in the chassis to which this command must apply.

Example The following command sets maximum partitions:

```
ACOS(config)#techreport max-partitions 50
Polling periodic techreport max-partitions is 50
```

Related Commands:

- cert-pinning

terminal

Description Set the terminal configuration.

Syntax

```
[no] terminal
{
auto-size |
editing |
gslb-prompt options |
history [size number] |
idle-timeout minutes |
length number |
prompt options |
width lines
}
```

Parameter	Description
auto-size	Automatically adjusts the length and width of the terminal display. Auto-sizing is enabled by default.

Parameter	Description

gslb-prompt *options*	Enables display of the ACOS device's role within a GSLB group at the CLI prompt.
	• **disable** - disables display of the GSLB group status.
	• **group-role symbol** - Displays "Member" or "Master" in the CLI prompt; for example:
	`ACOS:Master(config)#`
	• **symbol** - Displays "gslb" in the CLI prompt after the name of the ACOS device; for example:
	`ACOS-gslb:Master(config)#`

editing	Enables command editing. This feature is enabled by default.
history [**size** *number*]	Enables the command history and specifies the number of commands it can contain, 0-1000. By default, history is enabled for up to 256 commands.
idle-timeout *minutes*	Specifies the number of minutes a CLI session can be idle before it times out and is terminated, 0-60 minutes. To disable timeout, enter 0. The default idle timeout is 15 minutes.
length *number*	Specifies the number of lines to display per page, 0-512. To disable paging, enter 0. The default length is 24 lines.
prompt *hostname*	Display hostname in prompt.
width *lines*	Specifies the number of columns to display, 0-512. To use an unlimited number of columns, enter 0. The default width is 80 columns.

Mode Configuration mode

Example The following example sets the idle-timeout to 30 minutes:

```
ACOS(config)# terminal idle-timeout 30
```

tftp blksize

Description Change the TFTP block size.

Syntax

```
[no] tftp blksize bytes
```

Replace *bytes* with the Maximum packet length the ACOS TFTP client can use when sending or receiving files to or from a TFTP server. You can specify from 512-32768 bytes.

Default 32768 bytes

Mode Configuration mode

Usage Increasing the TFTP block size can provide the following benefits:

- TFTP file transfers can occur more quickly, since fewer blocks are required to a send a file.
- File transfer errors due to the server reaching its maximum block size before a file is transferred can be eliminated.

To determine the maximum file size a block size will allow, use the following formula:

1K-blocksize = 64MB-filesize

Here are some examples.

Block Size	Maximum File Size
1024	64 MB
8192	512 MB
32768	2048 MB

Increasing the TFTP block size of the ACOS device only increases the maximum block size supported by the ACOS device. The TFTP server also must support larger block sizes. If the block size is larger than the TFTP server supports, the file transfer will fail and a communication error will be displayed on the CLI terminal.

If the TFTP block size is larger than the IP Maximum Transmission Unit (MTU) on any device involved in the file transfer, the TFTP packets will be fragmented to fit within the MTU. The fragmentation will not increase the number of blocks; however, it can re-add some overhead to the overall file transmission speed.

If the ACOS device is a member of an aVCS virtual chassis platforms, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following commands display the current TFTP block size, increase it, then verify the change:

```
ACOS(config)# show tftp
TFTP client block size is set to 512
ACOS(config)# tftp blksize 4096
ACOS(config)# show tftp
TFTP client block size is set to 4096
```

timezone

Description Configure the time zone on your system.

Syntax

```
[no] timezone zone [nodst]
```

Parameter	Description
zone	Specify the time zone. Enter **timezone ?** at the CLI prompt to see a list of available time zones.
nodst	Disable daylight savings time adjustments for the time on your system.

Default GMT

Mode Configuration mode

Usage If you use the GUI or CLI to change the ACOS timezone or system time, the statistical database is cleared. This database contains general system statistics (performance, and CPU, memory, and disk utilization) and SLB statistics.

Example The following example sets the time zone to America/Los_Angeles. Daylight savings time adjustments will be made.

```
ACOS(config)# timezone America/Los_Angeles
```

tx-congestion-ctrl

Description Configure looping on the polling driver, on applicable models.

NOTE: This command can impact system performance. It is recommended not to use this command unless advised by technical support.

Syntax

```
tx-congestion-ctrl retries
```

You can specify 1-65535 retries.

Default 1

Mode Configuration mode

upgrade gui

Description Upgrade or rollback the Thunder device primary or secondary GUI image from the hard disk. Write the upgrade image to the hard disk by replacing the current image at that location.

Syntax

```
upgrade gui {pri | sec}
{delete | local | rollback | save-gui | show-percentage |
source-ip-address | upload | use-mgmt-port | url}
```

Parameter	Description
pri	Upload the GUI image on the primary hard disk.
sec	Replace the GUI image on the secondary hard disk.
delete *image-name*	Delete any one existing local GUI image.
local *image-name*	Specify the upgrade image filename from the local image repository. Use **show gui-image-list** to view a list of available local images.

Parameter	Description
	The *image-name* can be 1-128 characters.
rollback *image-name*	Rollback the specific GUI image on the Thunder Device. The image will be rolled back to the most recent version that was previously saved on the Thunder device. You can select the image from any available GUI images that was previously uploaded to the device's image repository, see upload url.
save-gui *url*	Save the GUI image on the remote server using the specified url .
show-percentage *url*	Enable this option to view the file transmit percentage for the specified url .
source-ip-address *ip address* **[save-gui** *url* **| show-percentage** *url* **| upload** *url* **|** *url***]**	Connect the remote server or device using the source IP address of the source interface and upload the primary or secondary image from the remote server. The following options are available under this command: • save-gui url • show-percentage url • upload url • url
upload *url*	Upload the GUI image from the remote server using the specified url . This option allows you to upload different versions of the GUI image to the Thunder device from local or remote server, provided that the System and GUI images are compatible. These images are then saved to the device's image

Parameter	Description
	repository for future use, such as upgrade or rollback. A maximum of five images can be uploaded for each hard disk partition (primary or secondary).
use-mgmt-port [save-gui *url* **| show-percentage** *url* **| upload** *url* **|** *url***]**	Connect the remote server or device using the management interface as the source port and upload the primary or secondary image from the remote server. To connect to the remote server, the management route table is utilised. By default, the ACOS device attempts to reach the remote server through a data interface using the data route table. The following options are available under this command: • save-gui url • show-percentage url • upload url • url
url	Specify the file path protocol, username (if required), and directory path to upload the image from the remote server or device. The transfer will be initiated from within Thunder, so network connectivity is required between the Thunder device and the remote server containing the image. On the command line, you can input the complete URL or press **Enter** to display a prompt for each component of the URL. To enter the entire URL:

Parameter	Description
	• tftp://*host*/*file* • ftp://[user@]host[:port]/file • scp://[*user*@]*host*/*file* • http://[*user*@]*host*/*file* • https://[*user*@]*host*/*file* • sftp://[*user*@]*host*/*file* If you enter the entire URL, you will prompted to specify the user name and/or password. The password can be up to 255 characters long. • The following special characters are supported in the password: !#$()*+,-.;=^_`{|}~ • The following special characters are not supported in the password: (blank space) "%&'/:<>?@[\]

Default N/A

Mode Global Configuration Mode

Usage For upgrading the image using GUI, see the *Online Help* for the ACOS release to which you plan to upgrade.

Example Below is an example output from a successful upgrade.

```
ACOS(config)# upgrade gui pri
scp://admin@192.168.1.1/packages/5_2_1-p6-5_2_1-P6-1.upg
Password []?

System configuration has been modified. Save? [yes/no]:yes
Building configuration...
Write configuration to primary default startup-config
[OK]
Running configuration is saved
```

```
Do you want to reboot the system after the upgrade?
[yes/no]:yes
Getting upgrade package ...
.....................................................
Done (0 minutes 59 seconds)
Decrypt upgrade package ...
.................... Done (0 minutes 21 seconds)
Checking integrity of upgrade package ...
 Upgrade file integrity checking passed (0 minutes 1 seconds)
Expand the upgrade package now ............ Done (0 minutes 10
seconds)
Upgrade .....................................................
Upgrade was successful (0 minutes 52 seconds)
Rebooting system ...
ACOS(config)#
```

upgrade hd

Description Upgrade or rollback the Thunder device primary or secondary image. Write the upgrade image to the hard disk by replacing the existing image at that location.

Syntax

```
upgrade hd {pri | sec}
{local image-name | rollback | show-percentage | source-ip-
address ip address | use-mgmt-port | url}
```

Parameter	Description
pri	Replace the primary image on the hard disk.
sec	Replace the secondary image on the hard disk.
local *image-name* [**reboot-after-upgrade** | **staggered-upgrade-mode Device** *device-id*]	Specify the upgrade image from the local VCS image repository. Use **show vcs images** to view a list of available local images. The *image-name* can be 1-128 characters and the format should be: `aximage_XX_XX_`

Parameter	Description
	`XX_XX.tar.gz.` The following options are available under this command: • reboot-after-upgrade • staggered-upgrade-mode Device device-id [reboot-after-upgrade]
reboot-after-upgrade	Reboot the system after the upgrade is complete.
staggered-upgrade-mode Device *device-id [reboot-after-upgrade]*	Use VCS staggered upgrade mode and specify the device ID (1-16 characters). If required, specify reboot-after-upgrade. A staggered upgrade avoids disruption of services during an image upgrade for those with aVCS setup. **NOTE:** It is recommended not to use this option unless explicitly stated to do so. For more information, see *Release Notes*.
rollback	Rollback the primary or secondary image on the Thunder Device. The image will be rolled back to the most recent version that was previously saved on the Thunder device. In the following scenarios, the **rollback** command is unavailable: • Platforms with 32 GB or less disk size, such as TH840/TH940/TH1040. • The available disk size is less than 8GB.
show-percentage *url*	Enable this option to view the file transmit

Parameter	Description
	percentage for the specified url {reboot-after-upgrade | staggered-upgrade-mode Device device-id [reboot-after-upgrade]}.
source-ip-address *ip address* **[show-percentage |** *url***]**	Connect the remote server or device using the source IP address of the source interface. The following options are available under this command: • show-percentage url • url {reboot-after-upgrade | staggered-upgrade-mode Device device-id [reboot-after-upgrade]}
use-mgmt-port [show-percentage | *url***]**	Connect the remote server or device using the management interface as the source port. To connect to the remote server, the management route table is utilised. By default, the ACOS device attempts to reach the remote server through a data interface using the data route table. The following options are available under this command: • show-percentage url • url {reboot-after-upgrade | staggered-upgrade-mode Device device-id [reboot-after-upgrade]}
url {**reboot-after-upgrade | staggered-upgrade-mode Device** *device-id [reboot-after-*	Specify the file path protocol, username (if required), and directory path to upload the image from the remote server or device. The transfer will be initiated from within

Parameter	Description
upgrade]}	Thunder, so network connectivity is required between the Thunder device and the remote server containing the image. On the command line, you can input the complete URL or press **Enter** to display a prompt for each component of the URL. To enter the entire URL: • `tftp://host/file` • `ftp://[user@]host[:port]/file` • `scp://[user@]host/file` • `http://[user@]host/file` • `https://[user@]host/file` • `sftp://[user@]host/file` If you enter the entire URL, you will be prompted to specify the user name and/or password. The password can be up to 255 characters long. • The following special characters are supported in the password: `!#$()*+,-.;=^_`{|}~`  • The following special characters are not supported in the password:  `(blank space) "%&'/:<>?@[\]` The following options are available under this command: • reboot-after-upgrade

Parameter	Description
	• staggered-upgrade-mode Device device-id [reboot-after-upgrade]

Default N/A

Mode Global configuration mode

Usage For complete upgrade instructions, see the *Release Notes* for the ACOS release to which you plan to upgrade.

Example The following output is an example of a successful ACOS image upgrade using SCP.

```
ACOS(config)# upgrade hd sec
scp://admin@192.168.1.1/packages/aximage_5_2_1-p6_43.tar.gz
Password []?

System configuration has been modified. Save? [yes/no]:yes
Building configuration...
Write configuration to primary default startup-config
[OK]
Running configuration is saved

Do you want to reboot the system after the upgrade?
[yes/no]:yes
Getting upgrade package ...
.....................................................
Done (0 minutes 59 seconds)
Decrypt upgrade package ...
.................. Done (0 minutes 21 seconds)
Checking integrity of upgrade package ...
 Upgrade file integrity checking passed (0 minutes 1 seconds)
Expand the upgrade package now ............ Done (0 minutes 10
seconds)
Upgrade .....................................................
Upgrade was successful (0 minutes 52 seconds)
Rebooting system ...
ACOS(config)#
```

Example The following output is an example of a successful ACOS image upgrade over SCP with Duo MFA enabled using direct passcode.

```
vThunder(config)# upgrade hd pri scp://path_to_ACOS_image.upg
Password []?

Do you want to reboot the system after the upgrade?[yes/no]:no
Getting upgrade package ...

Duo two-factor login for root

Enter a passcode or select one of the following options:

 1. Duo Push to XXX-XXX-6097
 2. SMS passcodes to XXX-XXX-6097 (next code starts with: 1)

Passcode or option (1-2): 656155


Authentication successful!
......
```

Example The following output is an example of a successful ACOS upgrade over SCP with Duo MFA enabled using push notification.

```
vThunder(config)# upgrade hd pri scp://path/ACOS_version.upg
```

```
Password []?
Do you want to reboot the system after the upgrade?[yes/no]:
no
Getting upgrade package ...
Duo two-factor login for root
Enter a passcode or select one of these options:
1. Duo Push to XXX-XXX-6097
2. SMS passcodes to XXX-XXX-6097

Passcode or option (1-2): 1

Authentication successful!
.................
Done (0 minutes 27 seconds)
Decrypting upgrade package...
```

Example The following output is an example of a successful ACOS image upgrade over SCP with Duo MFA enabled using SMS passcode.

```
vThunder(config)# upgrade hd pri scp://path_to_ACOS_image.upg
```

```
Password []?

Do you want to reboot the system after the upgrade?[yes/no]:no
Getting upgrade package ...

Duo two-factor login for root

Enter a passcode or select one of the following options:

 1. Duo Push to XXX-XXX-6097
 2. SMS passcodes to XXX-XXX-6097 (next code starts with: 1)

Passcode or option (1-2): 2
New SMS passcodes sent.
Duo two-factor login for root

Enter a passcode or select one of the following options:

 1. Duo Push to XXX-XXX-6097
 2. SMS passcodes to XXX-XXX-6097 (next code starts with: 1)

Passcode or option (1-2): 656155

Authentication successful!
......
```

vcs

Description Configure aVCS.

The **vcs** commands are available only when aVCS is enabled. To enable aVCS, use the **vcs enable** command.

For more information, see “aVCS CLI Commands” in *Configuring ACOS Virtual Chassis Systems*.

ve-stats

Description Enable statistics collection for Virtual Ethernet (VE) interfaces.

NOTE: This command does not work in L3V partitions.

Syntax

```
[no] ve-stats enable
```

Default Disabled

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

vlan

Description Configure a virtual LAN (VLAN). This command changes the CLI to the configuration level for the VLAN.

Syntax

```
[no] vlan vlan-id
```

Replace *vlan-id* with the ID of the VLAN (2-4094).

If the ACOS device is a member of an aVCS virtual chassis, specify the *vlan-id* as follows:

DeviceID/*vlan-id*

Default VLAN 1 is configured by default. All Ethernet data ports are members of VLAN 1 by default.

Mode Configuration mode

Usage You can add or remove ports in VLAN 1 but you cannot delete VLAN 1 itself.

Example The following command adds VLAN 69 and enters the configuration level for that VLAN:

```
ACOS(config)# vlan 69
ACOS(config-vlan:69)#
```

Example You cannot have duplicate VLANs configured across partitions. In this example, VLAN 10 is configured in the shared partition:

```
ACOS(config)# vlan 10
```

```
ACOS(config-vlan:10)# exit
ACOS(config)#
```

If you attempt to configure VLAN 10 in an L3V partition, you will receive an error message:

```
ACOS(config)# active-partition p2
Current active partition: p2
ACOS[p2]# configure
ACOS[p2](config)# vlan 10
This VLAN or Port is owned by another partition.
```

vlan-global enable-def-vlan-l2-forwarding

Description Enable Layer 2 forwarding on the default VLAN (VLAN 1).

Syntax

```
[no] vlan-global enable-def-vlan-l2-forwarding
```

Default Layer 2 forwarding is disabled on VLAN 1, on ACOS devices deployed in route mode.

Usage This command applies only to routed mode deployments.

On a new or unconfigured ACOS device, as soon as you configure an IP interface on any individual Ethernet data port or trunk interface, Layer 2 forwarding on VLAN 1 is disabled.

When Layer 2 forwarding on VLAN 1 is disabled, broadcast, multicast, and unknown unicast packets are dropped instead of being forwarded. Learning is also disabled on the VLAN. However, packets for the ACOS device itself (ex: LACP) are not dropped.

NOTE: Configuring an IP interface on an individual Ethernet interface indicates you are deploying in route mode (also called “gateway mode”). If you deploy in transparent mode instead, in which the ACOS device has a single IP address for all data interfaces, Layer 2 forwarding is left enabled by default on VLAN 1.

vlan-global l2-fwd-for-me-arp-ns

Description Enables Layer 2 forwarding for both ARP and NS packets with target IP/IPv6 addresses that are owned by the device.

Syntax `[no] vlan-global l2-fwd-for-me-arp-ns`

Default Forwarding ARP or IPv6 NS packets in any VLAN is disabled.

Usage This command enables forwarding the Broadcast packets to the other ports of a VLAN when the ARP/IPv6 NS packets received by ACOS have their target IP/IPv6 addresses owned by the devices.

Example The following command enables layer 2 forwarding for both ARP and NS packets:

```
ACOS(config)# vlan-global l2-fwd-for-me-arp-ns
```

vlan-global l3-vlan-fwd-disable

Description Globally disable Layer 3 forwarding between VLANs.

Syntax `[no] vlan-global l3-vlan-fwd-disable`

Default By default, the ACOS device can forward Layer 3 traffic between VLANs.

Usage This option is applicable only on ACOS devices deployed in gateway (route) mode. If the option to disable Layer 3 forwarding between VLANs is configured at any level, the ACOS device can not be changed from gateway mode to transparent mode, until the option is removed.

- Depending on the granularity of control required for your deployment, you can disable Layer 3 forwarding between VLANs at any of the following configuration levels:
- Global – Layer 3 forwarding between VLANs is disabled globally, for all VLANs. (Use this command at the Configuration mode level.)
- Individual interfaces – Layer 3 forwarding between VLANs is disabled for incoming traffic on specific interfaces.
- Access Control Lists (ACLs) – Layer 3 forwarding between VLANs is disabled for all traffic that matches ACL rules that use the **l3-vlan-fwd-disable** action.

web-service

Description Configures web services.

Syntax `[no] web-service options`

Parameter	Description
auto-redir	Enables requests for the unsecured port (HTTP) to be automatically redirected to the secure port (HTTPS). This feature is enabled by default.
axapi-session-limit *num*	Specifies the maximum number of aXAPI sessions that can be run simultaneously (1-100). The default is 30.
axapi-timeout-policy idle *minutes*	Specifies the number of minutes an aXAPI session or GUI session can remain idle before being terminated. Once the aXAPI session is terminated, the session ID generated by the ACOS device for the session is no longer valid. You can specify 0-60 minutes. If you specify 0, sessions never time out. The default timeout is 10 minutes.
axapi-token-sharing	Enables sharing of aXAPI token within multiple hosts without the need to authenticate the hosts. This feature is disabled by default. **NOTE:** If `axapi-token-sharing` is enabled and multiple sessions are created, the outside hosts can access ACOS with the token from any session.
gui-session-limit *num*	Specifies the maximum number of GUI sessions that can be run simultaneously (1-100). The default is 30.
gui-timeout-policy	Specifies the number of minutes GUI session

Parameter	Description
idle *minutes*	can remain idle before being terminated. Once the GUI session is terminated, the session ID generated by the ACOS device for the session is no longer valid. You can specify 0-60 minutes. If you specify 0, sessions never time out. The default timeout is 10 minutes.
keep-alive-timeout *seconds*	Specifies the time (in seconds) before an idle keep-alive connections are closed. You can specify 1-65535 seconds. The default timeout is 30 seconds.
login message *characters*	Specify the GUI login message (1-1985).
max-keep-alive-requests *num*	Specifies the maximum number of requests allowed per connection when keep-alive is on. You can specify 0-65535. If it is set to 0, unlimited requests will be allowed. The default is 100.
mpm-max-conn *<num>*	Specify the number to set the maximum concurrency. The number indicates how many HTTP worker processes can be launched at the same time.
mpm-max-conn-per-child *num*	Specify the number to set a maximum number of connections each worker process will handle. After that, the worker process retires. This avoids potential memory leaks. A smaller number means the worker process will launch and quit frequently, causing low performance.
mpm-min-spare-	Specify the number to set minimum spare

Parameter	Description
conn *num*	worker processes. A bigger number means more TCP connections can be established initially. The number should be less than the `mpm-max-conn`. Otherwise, the real value will be the same as `mpm-max-conn`.
port *port*	Specifies the port number for the unsecured (HTTP) port. The default HTTP port is 80.
pre-login-message *num*	Specify the pre GUI login message (1-1985).
public-apis /axapi/v3/<sub path>	Specify the public APIs which can be called without authentication and authorization. **NOTE:** Do not set critical APIs for security consideration.

secure	Generate a new certificate for your ACOS device when it is booted for the first time.
	
	Use the **certificate** or **private-key** parameters to load an externally-generated certificate or private-key. For the URL, you can specify:
	
	• certificate: used to load an externally-generated certificate. For the URL, you can specify:
	  ◦ `tftp://host/file`
	  ◦ `ftp://[user@]host[port:]/file`
	  ◦ `scp://[user@]host/file`
	  ◦ `sftp://[user@]host/file`
	• generate: used for secure certificate generation. You must specify the domain

Parameter	Description
	name, and can optionally specify the country and state location. • private-key: used to load an externally-generated private-key. • regenerate: used for secure certificate re-generation. You must specify the domain name, and can optionally specify the country and state location. • restart: used for restarting the web service. • wipe: used to wipe the web private-key and certificate.
secure-port *port*	Specifies the port number for the secure (HTTPS) port. The default HTTPS port is 443.
secure-server disable	Disables the HTTPS server. This server is enabled by default.
server disable	Disables the HTTP server. This server is enabled by default.

Mode Configuration mode

Usage If you disable HTTP or HTTPS access, any sessions on the management GUI are immediately terminated.

For more information, see the following:

- "Configuring Web Access" chapter of the *Management Access and Security Guide*
- "Configuring Basic System Parameters" chapter of the *System Configuration and Administration Guide*

Example The following command disables management access on HTTP:

```
ACOS(config)# web-service server disable
```

Example The following command enables the aXAPI token sharing within multiple hosts:

```
ACOS(config)# web-service axapi-token-sharing
```

write

Description Write the current running-config.

Related Commands:

- write force
- write memory
- write terminal

Show Commands

show access-list

Description Displays the configured IPv4 or IPv6 Access Control Lists (ACLs). The output lists the configuration commands for the ACLs in the running-config.

Syntax

```
show access-list { ipv4 [acl-id | acl_name] binding | ipv6 acl_name }
```

Parameter	Description
ipv4 [*acl-id* | *acl_name*] binding	Specify the IPv4 ACL by its ID or by its name. binding - Specify interfaces or ports associated with IPv4 ACLs.
ipv6 *acl_name*	Specify the IPv6 ACL by its name.

Mode All

Example The following command displays the information about the IPv4 access control list (ACL) with the ID number 1:

```
ACOS# show access-list ipv4 1
```

```
access-list 1 permit 198.162.11.0 0.0.0.255 Data plane hits: 3
access-list 1 deny 198.162.12.0 0.0.0.255 Data plane hits: 1
```

Example The following command displays the information about the management plane hits for IPv4 ACL with the ID number 50:

NOTE: The management hit count is displayed only when the ACL is bound to the management interface or if the enable-management command is used to bind the ACL to the management interface.

```
ACOS# show access-list ipv4 50
Management hit count: 175
access-list 50 permit 198.162.12.0 0.0.0.255 Data plane hits:
0, Management plane hits: 175
```

Example The following command displays the information about the management plane hits for IPv6 ACL with the name acl1:

```
ACOS# show access-list ipv6 acl1
Management hit count: 0
ipv6 access-list acl1
4 permit icmp host 2001::10 any Data plane hits: 0 ,
Management plane hits: 0
8 permit ipv6 host 2001::12 any Data plane hits: 0 ,
Management plane hits: 0
```

show acos-events messages

Description Displays the acos events messages.

Syntax

```
show acos-events messages
{
active-msgs |
all-msgs |
message-id | interface
}
```

Parameter	Description
active-msgs	Shows all the logs enabled by acos-events configuration.

Parameter	Description
all-msgs	Shows all logs in the system.
message-id	Shows all logs under the provided message-id as the following: `acos-events message-id <message-id> all/node-only/children-only/log-field-only` • `all` - Shows logs at this level and all sub-trees. • `node-only` - Shows logs at this node only. • `children-only` - Shows logs from all its sub-trees. • `log-field-only` - Shows complete details for a specific log: Select if the message-id indicates a specific log. **NOTE:** Select log-field-only if the provided message-id is log-field. • `<message-id>` can be taken from '`show acos-events all-msgs`' output. The whole Log ID in that output is a log-field, but parts of it are the actual object lineages leading to that log-field. For example, in '`interface.management.port-state`' , the entire text is a log-field, but '`interface`' and '`interface.management`' are object lineages leading to the log-field which might have more than one log-fields under them.
interface	• *`all`* - Shows logs at this level and all sub-trees. • *`node-only`* - Shows logs at this node only. • *`children-only`* - Shows logs from all its sub-trees. • *`log-field-only`* - Shows only this log: Select if the message-id indicates a specific log.

Parameter	Description	
	NOTE:	Select log-field-only if the provided message-id is log-field.

Mode All

Example The following command displays all messages when acos-events is activated enabling all logs:

```
ACOS# show acos-events messages all-msgs
------------------------------------------------------------------
-----------------                 ----------------------------
---------------------------
Note: Also displays the collector groups that enabled the
logs/formats
Log ID  SYSLOG CEF  LEEF
------------------------------------------------------------------
-----------------                 ----------------------------
---------------------------
Total logs = 983
------------------------------------------------------------------
-----------------                 ----------------------------
---------------------------
chassis-infra.blade-reboot Local+Remote   Not-defined
Not-defined
cg1
plat-buff-stats.core-crc-action Local+Remote   Not-defined
    Not-defined
cg1
reboot.restart  Local+Remote  Not-defined         Not-defined
cg1
interface.management.port-state  Local+Remote Disabled
   Disabled
cg1
slb.resource-usage.slb_threshold_cross  Local+Remote Disabled
          Disabled
cg1
slb.template.client-ssl.log-ssl-alert  Local+Remote Disabled
         Disabled
```

```
cg1
system.fast-aging-disabled Local+Remote   Not-defined
Not-defined
cg1
system.prof-parse-err   Local+Remote Not-defined         Not-
defined
cg1
system.prof-link-failed  Local+Remote Not-defined         Not-
defined
cg1
system.acos-shutdown-failed   Local+Remote  Not-defined
 Not-defined
--MORE--
```

The running-config is as follows:

```
ACOS(config)#show running-config acos-events
!Section configuration: 417 bytes
!
acos-events message-selector ms1
 rule 1
   message-id cmroot all
!
acos-events log-server ls1 1.1.1.2
  health-check-disable
  port 514 udp
    health-check-disable
!
acos-events collector-group cg1 udp
  log-server ls1 514
!
acos-events template t1
  message-selector ms1
    collector-group cg1
!
acos-events active-template t1
!
```

The following command displays active messages when acos-events is activated and enabled only interface.ethernet logs

```
ACOS(config)#show acos-events messages active-msgs
------------------------------------------------------------
                                  ------------------------------
--------------------------
Note: Also displays the collector groups that enabled the
logs/formats
Log ID  SYSLOG   CEF    LEEF
------------------------------------------------
                                  ------------------------------
--------------------------
Total logs = 983
Active logs = 3
------------------------------------------------------------------
------------------              ------------------------------
---------------------------
interface.ethernet.port-state Local+Remote  Disabled
Disabled
cg1
interface.ethernet.icmp_exceed  Local+Remote Disabled
Disabled
cg1
interface.ethernet.icmpv6_exceed Local+Remote Disabled
Disabled
cg1
```

The running-config is as follows:

```
ACOS(config)# show running-config acos-events
!Section configuration: 429 bytes
!
acos-events message-selector ms1
rule 1
message-id interface.ethernet all
!
acos-events log-server ls1 1.1.1.2
health-check-disable
port 514 udp
health-check-disable
!
```

```
acos-events collector-group cg1 udp
log-server ls1 514
!
acos-events template t1
message-selector ms1
collector-group cg1
!
acos-events active-template t1
!
```

The following command shows all logs under a specific message-id (it can be object or the log-field)

a. message-id as object:

```
ACOS(config)#$ show acos-events messages message-id
interface.ve all
-----------------------------------------------------------------
-                                  ----------------------------
---------------------------
Note: Also displays the collector groups that enabled the
logs/formats
Log ID  SYSLOG  CEF   LEEF
-----------------------------------------------------------------
------------------                 ----------------------------
---------------------------
interface.ve.icmpv6_exceed Disabled Disabled  Disabled

interface.ve.icmp_exceed  Disabled  Disabled  Disabled

interface.ve.state   Disabled  Disabled  Disabled
```

The following command shows the details log message log-field-only is selected:

```
ACOS(config)# show acos-events messages message-id
interface.ve.state log-field-only
Log                 interface.ve.state
Descriptive Name    Virtual Interface Status Change
Signature           (null)
```

```
Trigger              VE interface state change
Defined Severity     6
Configured Severity  6
Importance           2
Rate-limiting        Enabled
Defined-route        Local+Remote
Configured-route     none
Log Details:
Log-name             SYSLOG
Local-logging-conf   Disabled
Remote-logging-conf  Disabled
Log-format           Virtual Ethernet interface %s  is %s

Log-name             CEF
Local-logging-conf   Disabled
Remote-logging-conf  Disabled
Log-format           cs1=%s cs1Label=Virtual Ethernet Interfa

           ce cs2=%s cs2Label=VE Interface State

Log-name             LEEF
Local-logging-conf   Disabled
Remote-logging-conf  Disabled
Log-format           Virtual_Ethernet_Interface=%s VE_
Interface_State=%s
```

show active-partition

Description This command is described in the *Configuring Application Delivery Partitions* guide.

show admin

Description Display the administrator accounts.

Syntax

```
show admin [admin-name] [detail | session]
```

Parameter	Description
admin-name	Administrator name.
detail	Shows detailed information about the admin account.
session	Shows the current management sessions.

Mode Privileged EXEC mode and configuration mode

Example The following command lists the admins configured on an ACOS Device:

```
ACOS# show admin
Total number of configured users:  8
   Privilege     R: read-only, W: write, P: partition, En:
Enable
   Access Type   C: cli, W: web, A: axapi

UserName                        Status    Privilege Access
Partition
-----------------------------------------------------------
-----
admin                           Enabled   R/W       C/W/A
admin1                          Enabled   R/W       W
admin2                          Enabled   R         C/W/A
CorpAadmin                      Enabled   P.En      C/W/A
companyA
CorpBadmin                      Enabled   P.R/W     C/W/A
companyB
```

The following table describes the fields in the command output.

Field	Description
UserName	Name of the ACOS admin.
Status	Administrative status of the account.
Privilege	Access privilege level for the account: • R/W – Read-write. Allows access to all levels of the system.

Field	Description
	• R – Read-only. Allows monitoring access to the system but not configuration access. In the CLI, this account can only access the User EXEC and Privileged EXEC levels, not the configuration levels. In the GUI, this account cannot modify configuration information. • P.R/W – The admin has read-write privileges within the L3V partition to which the admin has been assigned. The admin has read-only privileges for the shared partition. • P.R – The admin has read-only privileges within the L3V partition to which the admin has been assigned, and read-only privileges for the shared partition. • P.En– The admin is assigned to an L3V partition but has permission only to view service port statistics for real servers in the partition, and to disable or re-enable the real servers or their service ports. **NOTE:** The "P" (partition) privilege levels apply to Application Delivery Partitions (ADP). For more information, see *Configuring Application Delivery Partitions* guide.
Access	Which modules the admin is allowed to access: • C - Admin is allowed CLI access. • W - Admin is allowed web (GUI) access. • A - Admin is allowed aXAPI access.
Partition	L3V partition to which the admin is assigned.

Example The following command lists details for the "admin" account:

```
ACOS# show admin admin detail
  User Name              ...... admin
```

```
Status                  ...... Enabled
Privilege               ...... R/W
Partition               ......
Access type               .....cli web axapi
GUI role              ......
Trusted Host(Netmask) ...... Any
Lock Status             ...... No
Lock Time               ......
Unlock Time             ......
```

The following table describes the fields in the command output.

Field	Description
User Name	Name of the ACOS admin.
Status	Administrative status of the account.
Privilege	Access privilege level for the account: • R/W – Read-write. Allows access to all levels of the system. • R – Read-only. Allows monitoring access to the system but not configuration access. In the CLI, this account can only access the User EXEC and Privileged EXEC levels, not the configuration levels. In the GUI, this account cannot modify configuration information. • Partition-write – The admin has read-write privileges within the private partition to which the admin has been assigned. The admin has read-only privileges for the shared partition. • Partition-read – The admin has read-only privileges within the private partition to which the admin has been assigned, and read-only privileges for the shared partition. • Partition-enable-disable – The admin is assigned to a private partition but has permission only to

Field	Description
	view service port statistics for real servers in the partition, and to disable or re-enable the real servers and their service ports.
Partition	Private partition to which the admin is assigned. **NOTE:** A partition name appears only for admins with Partition-write, Partition-read, or Partition-enable-disable privileges. For other privilege levels, this field is blank.
Access type	Management interfaces the admin is allowed to access, which can be one or more of the following: • cli • web • axapi
GUI role	Role assigned to the admin for GUI access. **NOTE:** If the admin is configured using the GUI, assignment of a role is required. However, if the admin is configured using the CLI, a GUI access role can not be assigned. In this case, the GUI role is equivalent to ReadWriteAdmin.
Trusted Host (Netmask)	IP host or subnet address from which the admin must log in.
Lock Status	Indicates whether the admin account is currently locked.
Lock Time	If the account is locked, indicates how long the account has been locked.
Unlock Time	If the account is locked, indicates how long the account will continue to be locked.

Example The following command lists all the currently active admin sessions:

```
ACOS# show admin session
```

```
Id     User Name    Start Time                        Source IP
  Type Partition Authen  Role            Cfg
-------------------------------------------------------------------
-----------------------------------------------
 2      admin        11:35:49 IST Tue Sep 30 2014  127.0.0.1
   WEBSERVICE          Local    ReadWriteAdmin  No
*4      admin        11:43:12 IST Tue Sep 30 2014  172.17.0.224
   CLI              Local    ReadWriteAdmin  No
```

The following table describes the fields in the command output.

Field	Description
Id	Admin session ID assigned by the ACOS Device. The ID applies only to the current session.
User Name	Admin name.
Start Time	System time when the admin logged onto the ACOS Device to start the current management session.
Source IP	IP address from which the admin logged on.
Type	Management interface through which the admin logged on.
Partition	Partition that is currently active for the management session.
Authen	Indicates the database used to authenticate the admin: • Local – Admin database on the ACOS Device • RADIUS – Admin database on a RADIUS server • TACACS – Admin database on a TACACS+ server
Role	Indicates the role assigned to the admin for GUI access.
Cfg	Indicates whether the admin is at the configuration level.

show aflex

Description Display the configured aFlex scripts.

Syntax `show aflex [aflex-name] [all-partitions | partition name]`

Mode All

Usage To display the aFleX policies for a specific partition only, use the `partition name` option.

Example The following command shows the aFlex scripts on an ACOS Device:

```
ACOS# show aflex
Total aFleX number: 6
Name                                Syntax   Virtual port
------------------------------------------------------------
aFleX_Remote                        No       No
aFleX_check_agent                   No       No
aFleX_relay_client                  Check    No
bugzilla_proxy_fix                  Check    Bind
http_to_https                       Check    No
louis                               No       No
```

The following table describes the fields in the command output.

Field	Description
Total aFleX number	Total number of aFlex scripts on the ACOS Device.
Name	Name of the aFleX policy.
Syntax	Indicates whether the aFleX policy has passed the syntax check performed by the ACOS Device: Check – The aFleX policy passed the syntax check. No – The aFleX policy did not pass the syntax check.
Virtual port	Indicates whether the aFleX policy is bound to a virtual port.

show arp

Description Display ARP table entries.

Syntax

```
show arp [all | ipv4-address | ipv6-address]
```

Mode All

Example The following command lists the ARP entry for host 61.61.61.100:

```
ACOS(config)# show arp 61.61.61.100
Total arp entries: 1            Age time: 300 secs
IP Address      MAC Address      Type     Age    Interface
Vlan/Encap
-----------------------------------------------------------------
-----------
61.61.61.100    021f.a000.00f8   Dynamic  45     lif 100
1

vtep info
---------
vtep id: 100  age: 45  partition id: 0     static: No    encap
type: GRE
local: 30.1.1.2        remote: 10.1.1.100
```

The following table describes the fields in the command output.

Field	Description
Total arp entries	Total number of entries in the ARP table. This total includes static and learned (dynamic) entries.
Age time	Number of seconds a dynamic ARP entry can remain in the table before being removed.
IP Address	IP address of the device.
MAC Address	MAC address of the device.
Type	Indicates whether the entry is static or dynamic.
Age	Number of seconds since the entry was last used in

Field	Description
	the dynamic entries.
Interface	ACOS interface through which the device that has the displayed MAC address and IP address can be reached.
Vlan/Encap	VLAN or encapsulated tunnel through which the device that has the MAC address can be reached.
vtep info	Overlay tunnel endpoint information.

show audit

Description Show the command audit log.

Syntax

```
show audit [all-partitions | partition {shared | name}]
```

Mode All

Usage The audit log is maintained in a separate file, apart from the system log. The audit log messages that are displayed for an admin depend upon the admin's privilege level:

- Admins with Root, Read Write, or Read Only privileges who view the audit log can view all the messages, for all system partitions. To display the messages for a specific partition only, use the **partition** option.
- Admins who have privileges only within a specific partition can view only the audit log messages related to management of that partition. Admins with partition-enable-disable privileges can not view any audit log entries.

Example Below is a sample output of the command audit log (truncated for brevity):

```
ACOS# show audit
Sep 30 2014 11:54:26  [admin] cli: [172.17.0.224:60009] show
audit
Sep 30 2014 11:54:22  [admin] axapi: [1412074462810894] RESP
HTTP status 200 OK
```

```
Sep 30 2014 11:54:22  [admin] axapi: [1412074462810894] GET:
/axapi/v3/system/ctrl-cpu/oper
Sep 30 2014 11:54:22  [admin] axapi: [1412074462808372] RESP
HTTP status 200 OK
Sep 30 2014 11:54:22  [admin] axapi: [1412074462808372] GET:
/axapi/v3/system/memory/oper
Sep 30 2014 11:54:22  [admin] axapi: [1412074462804830] RESP
HTTP status 200 OK
```

show automatic-update

Description Displays the updated CA bundle, application firewall protocol bundle, and A10 Threat Intel details.

Syntax

```
show automatic-update
```

Mode All

Example The following command lists the schedule update details:

```
ACOS# show automatic-update
Feature name  Version     Schedule  Time   Last Updated  Next
Check
-----------------------------------------------------------------
app-fw        1.360.0-23    N/A     00:00  N/A           N/A
ca-bundle     20200722      N/A     00:00  2020-09-08    N/A
a10-threat-intel 20210329090521 Daily 02:24  2021-03-24
2021-03-24
central-cert-pin-list 20201216-1 Daily00:00  2020-12-15
2020-12-16
```

The following table describes the fields in the command output:

Field	Description
Feature Name	The name of the feature. It can have one of the following values: • app-fw • ca-bundle

Field	Description
	• a10-threat-intel
Version	The latest version of the feature.
Schedule	The daily or weekly schedule.
Time	The time when the schedule was executed.
Last Updated	The date when the feature version was last updated.
Next Check	The next schedule date.

show axdebug capture

Description Displays a list of axDebug captured packet files.

Syntax

```
show axdebug capture [partition name] [file-name]
```

Parameter	Description
`partition name`	Displays files only for a select partition.
file-name	Filters the show output for only files that partially match a specified *file-name*. It can be a length of 1-63.

Mode All

Example The following command displays the list of axDebug captured packet files on the device:

```
ACOS(axdebug)# show axdebug capture
-----------------------------------+-------------+----------
-----------------
Filename      | Size(Byte) | Date
-----------------------------------+-------------+----------
-----------------
file1         | 58801      | Tue Aug 23 22:49:07 2022
file123       |   192      | Fri Aug 26 17:06:51 2022
file456       |   288      | Mon Sept 5 10:34:55 2022
```

```
-----------------------------------+-------------+----------
------------------
Total: 3
Maximum file number is: 100
```

show axdebug config

Description Displays the axDebug filter configuration currently applied on ACOS.

Syntax

```
show axdebug config
```

Mode All

Example This example shows the output of the `show axdebug config` command:

```
ACOS(config)# show axdebug config
timeout 5
no incoming
no outgoing
count 3000
length 1518
file-size 1000
```

show axdebug config-file

Description Displays a list of the axDebug configuration files.

Syntax

```
show axdebug config-file [filename]
```

Mode All

Example The following example displays the details of the config-file named "file10":

```
ACOS(axdebug)#show axdebug config-file file10
AXDebug Config File : file10
-------------------------------------------------------------
!
end
!
active-partition shared
```

```
!
clear axdebug-filters
!
!
axdebug
 count 3000
 incoming
 outgoing
 length 1518
 maxfile 100
 timeout 5
 filter-config 1
  ip 10.211.1.132 192.0.0.0
  port 80 80
  proto tcp
  exit
pcapng-config
 pcapng-enable
 ssl-key-enable
```

show axdebug file

Description Display AX debug capture files or their contents.

Syntax `show axdebug file [parameters]`

Parameter	Description
`partition` *name*	Displays files only for a select partition.
filename	Filters the show output for only files that partially match a specified filename. • `datacpu` - specify a data CPU to show • `format` - Specify which format to show: • `hex` HEX format • `hexl2` HEX format with l2 header

Parameter	Description
	• `hexascii` HEX & ASCII format • `hexasciil2` HEX & ASCII format with l2 header • `ascii` ASCII format • `l2` With l2 header • `verbose` Verbose • `verbose1` More verbose • `verbose2` More more verbose • `timeno` Without time • `timedelta` Show delta time • `timeformat` Show standard time format

Mode All

Example The following command displays the list of AX debug capture files on the device:

```
ACOS(axdebug)# show axdebug file
-----------------------------------+--------------+----------
------------------
Filename                           |   Size(Byte) | Date
-----------------------------------+--------------+----------
------------------
file1                              |        58801 | Tue Sep
23 22:49:07 2008
file123                            |          192 | Fri Sep
26 17:06:51 2008
-----------------------------------+--------------+----------
------------------
Total: 2
Maximum file number is: 100
```

Example The following command displays the packet capture data in file “file123”:

```
ACOS(axdebug)# show axdebug file file123
```

```
Parse file for cpu #1:

Parse file for cpu #2:

15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: S
2111796945:2111796945(0) ack 3775149588 win 5792 <mss
1460,sackOK,timestamp 1368738447 524090233,nop,wscale 7>
15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: S
2111796945:2111796945(0) ack 3775149588 win 5792 <mss
1460,sackOK,timestamp 1368738447 524090233,nop,wscale 7>
15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: . ack
150 win 54 <nop,nop,timestamp 1368738447 524090233>
15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: . ack
150 win 54 <nop,nop,timestamp 1368738447 524090233>
15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: P
1:192(191) ack 150 win 54 <nop,nop,timestamp 1368738447
524090233>
15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: P
1:192(191) ack 150 win 54 <nop,nop,timestamp 1368738447
524090233>
15:16:05.788530 IP 10.10.11.30.http > 30.30.31.30.13649: F
192:192(0) ack 151 win 54 <nop,nop,timestamp 1368738448
524090234>
```

show axdebug filter

Description Displays the configured axDebug output filters.

Syntax **show axdebug filter** [*filter-num*]

Mode All

show axdebug status

Description Displays per-CPU packet capture counts for axDebug.

Syntax **show axdebug status** [*cpu-num* [...]]

Mode All

Example The following example shows the output for the `show axdebug status` command for all CPUs:

```
ACOS(config)#show axdebug status
tcpdump filter disabled
axdebug is disabled
session filter is enabled
pcapng is enabled.
pcapng sslkey is enabled.
300 seconds left
debug incoming interface 1
debug outgoing interface 2 3 5 8 9 10 11 12
maximum 3000 packets
Captured packet length 1111
cpu#1 captured 4 packets.
cpu#2 captured 1 packets.
cpu#3 captured 8 packets.
cpu#4 captured 1 packets.
cpu#5 captured 0 packets.
cpu#6 captured 6 packets.
```

show backup

Description Display information about scheduled backups.

Syntax

```
show backup
```

Mode All

Example The outputs for `show backup` command on ACOS devices.

```
ACOS#show backup
backup periodically system hour 1680 use-mgmt-port
scp://root@10.6.12.201/root/test_periodic_backup.
Last backup(11:15 GMT Wed Nov 29 2017) successfully.
Next backup will occur at 11:15 GMT Wed Feb 7 2018.
```

NOTE: Data displayed for the "`show backup`" CLI output has been consolidated to provide a single output for Multi-PU platforms.

show bfd

Description Displays information for Bidirectional Forwarding Detection (BFD).

Syntax

```
show bfd {neighbors [detail] | statistics}
```

Parameter	Description
neighbors	Displays summarized information for BFD neighbors.
detail	Displays detailed information for BFD neighbors.
statistics	Displays overall statistics for BFD packets.

Mode All

Example The following command displays the BFD neighbor status.

NOTE: If the BFD sessions are Micro-BFD, then the interface (trunk member port) name will be added next to the ACOS interface (Our Address).

```
ACOS#show bfd neighbors
Our Address      Neighbor Address  State  Holddown txint mult
diag
10.10.10.1(eth1) 9.1.1.2           Up     6000     1000    6
0/0
10.10.10.1(eth2) 9.1.1.2           Up     6000     1000    6
0/0

Our Address      Neighbor Address  State   Holddown txint mult
diag
2001:1::1 (eth3) 2001:1::2         Up      400      100    4
0/0
2001:1::1 (eth4) 2001:1::2         Up      400      100    4
0/0
```

The following table describes the fields in the command output.

Field	Description
Our Address	ACOS interface associated with the BFD session. The interface (trunk member port) name is added if the BFD sessions are Micro-BFD.
Neighbor Address	Neighbor interface associated with the BFD session.
State	Shows the local state of the session.
Holdtime	Maximum amount of time the ACOS waits for a BFD control packet from the neighbor.
txint	Configured interval at which the ACOS sends BFD control packets to the neighbor.
mult	Maximum number of consecutive times the ACOS will wait for a BFD control packet from the neighbor.
diag	Diagnostic codes for the local and remote ends of the BFD session.

Example The following command displays detailed BFD neighbor status:

```
ACOS#show bfd neighbors detail
Our Address 60.60.60.60
Neighbor Address 60.60.60.1
Clients TRUNK
Singlehop, Echo disabled, Demand disabled, UDP source port
49158
Asynchronous mode, Authentication None
CPU ID 1, Rx CPU ID 5, Interface index 10
Local State Up, Remote State Up, 0h:10m:35s up
Local discriminator 0x00000007, Remote discriminator
0x0000000e
Config DesiredMinTxInterval 800 milliseconds,
RequiredMinRxInterval 800 milliseconds
Local DesiredMinTxInterval 800 milliseconds,
RequiredMinRxInterval 800 milliseconds
Remote DesiredMinTxInterval 800 milliseconds,
RequiredMinRxInterval 800 milliseconds
Local Multiplier 4, Remote Multiplier 4
```

```
Hold Down Time 3200 milliseconds, Transmit Interval 800
milliseconds
Local Diagnostic: No Diagnostic(0)
Remote Diagnostic: No Diagnostic(0)
Last sent echo sequence number 0x00000000
Control Packet sent 859, received 856
Echo Packet sent 0, received 0
Inter-Packet Gap (ms):
Sent :272 740 732 732 776 748 712 776 732 788
Received :648 768 788 680 716 724 724 760 784 688
Dcmsg sent 2 Dcmsg rcvd 2
Session UP 0 times DOWN 0 times
```

The following table describes the fields in the command output.

Field	Description
Our Address	ACOS interface associated with the BFD session.
Neighbor Address	Neighbor interface associated with the BFD session.
Clients	Protocol that initiates this BFD session. It can be one or more of the following: Static, Trunk, OSPFv2, OSPFv3, IS-IS, or BGP.
Singlehop (or Multihop)	BFD session can be either singlehop or multihop.
Echo	Indicates whether Echo functionality has been enabled or disabled.
Demand	Indicates whether Demand mode functionality has been enabled or disabled.
UDP source port	UDP source port used for this BFD session.
Asynchronous mode (or Demand) mode	If configured and running, indicates whether BFD is operating in Asynchronous mode or Demand mode.

Field	Description
Authentication	Authentication method. This can be either “None” (if it is not configured) or one of the following supported authentication schemes: • Simple password • Keyed MD5 • Meticulous Keyed MD5 • Keyed SHA1 • Meticulous Keyed SHA1
CPU ID	Since BFD traffic is distributed across multiple data CPUs, this CPU ID refers to the one associated with the current BFD session.
Rx CPU ID	Shows the CPU ID per session that received the last BFD packet.
Interface index	Interface index associated with the current BFD session.
Local State	Shows the local state the session. The state can be one of the following: • Init • Up • AdminDown • Down
Remote State	Shows the remote state the session. The state can be one of the following: • Init • Up • AdminDown

Field	Description
	• Down
Local discriminator	The local discriminator value that the ACOS Device assigns for the current BFD session.
Remote discriminator	The remote discriminator value that the neighboring router claims.
Config	The configured timer values.
Local	The configured timer values sent in the last BFD control packet. This value is determined based on BFD package exchange and negotiation.
Remote	The timer values received in the last BFD control packet from the BFD neighbor.
Local Multiplier	The local multiplier sent in the last BFD packet.
Remote Multiplier	The remote multiplier received in the last BFD packet from the neighbor.
Hold Down Time	The expiration time after which the BFD session will be brought down. This value is determined with the negotiated interval value and the remote multiplier value.
Transmit Interval	The periodic interval to send BFD control packets.
Local Diagnostic:	The diagnostic value sent in the last BFD control packet.
Remote Diagnostic:	The diagnostic value received in the last BFD control packet from the neighbor.
Last sent echo sequence number	A10 Network's proprietary sequence number sent in the last echo packet.
Control Packet	Statistics of control packets for this BFD

Field	Description
sent....received	session.
Echo Packet sent...received	Statistics of echo packets received for this BFD session.
Inter-Packet Gap (ms).....Sent....Received	Inter packets time delay for the last 10 sent and received packets per BFD session.
Dcmsg....Sent...Rcvd	Messages sent from RX CPU to CPU during session management.
Session UP....DOWN	Number of times the session goes up or down.

Example

The following command shows BFD statistics:

```
ACOS(config)# show bfd statistics
IP Checksum error                          0
UDP Checksum error                         0
No session found with your_discriminator 39958
Multihop config mismatch                   0
BFD Version mismatch                       0
BFD Packet length field is too small       0
BFD Packet data is short                   0
BFD Packet DetectMult is invalid           0
BFD Packet Multipoint is invalid           0
BFD Packet my_discriminator is invalid     0
BFD Packet TTL/Hop Limit is invalid        0
BFD Packet auth length is invalid          0
BFD Packet auth mismatch                   0
BFD Packet auth type mismatch              0
BFD Packet auth key ID mismatch            0
BFD Packet auth key mismatch             103
BFD Packet auth seq# invalid               0
BFD Packet auth failed                     0
BFD local state is AdminDown               2
BFD Destination unreachable                1
BFD Other error                            0
```

The following table describes the fields in the command output.

Field	Description
IP Checksum error	Number of BFD packets that had an invalid IP checksum.
UDP Checksum error	Number of BFD packets that had an invalid UDP checksum.
No session found with your_ discriminator	Number of BFD packets whose Your Discriminator value did not match a My Discriminator value on the ACOS.
Multihop config mismatch	A multihop configuration mismatch occurs when an ACOS receives a BFD packet with a source or destination that matches an existing BFD session. It can also be caused in two other scenarios: • Local is configured as singlehop, but the packet is received on the UDP port for multihop. • Local is configured as multihop, but packet is received on the UDP port for singlehop.
BFD Version mismatch	Number of BFD packets with a different BFD version than the one in use by the ACOS.
BFD Packet length field is too small	Number of BFD packets whose Length field value was shorter than the minimum BFD packet length (24 bytes without authentication or 26 bytes with authentication).
BFD Packet data is short	The packet payload size is smaller than the BFD length value.
BFD Packet DetectMult is invalid	The value of the received DetectMult is “0”.
BFD Packet Multipoint is invalid	The value of the received multipoint flag is set to “1”.

Field	Description
BFD Packet my_ discriminator is invalid	Number of BFD packets whose My Discriminator value was invalid.
BFD Packet TTL/Hop Limit is invalid	In a singlehop BFD session, the IP time-to-live or IPv6 hop limit value must be 255. If a value other than 255 is detected, this field is incremented.
BFD Packet auth length is invalid	The BFD length without the BFD packet header does not match the expected authentication length byte value. The number of BFD control packets have wrong authentication lengths in bytes
BFD Packet auth type mismatch	Number of BFD packets carrying an authentication type that does not match the BFD authentication type configured on the ACOS.
BFD Packet auth key ID mismatch	This field is incremented when the key ID in the authentication header does not match the one configured on the ACOS.
BFD Packet auth key mismatch	This field is incremented when the received authentication key does not match the one configured on the ACOS.
BFD Packet auth seq# invalid	This field is incremented when the received authentication sequence number is not equal to or greater than the sequence number received previously.
BFD Packet auth failed	Number of BFD packets with an incorrect authentication value.
BFD local state is AdminDown	Number of BFD packets received while the BFD session was administratively down.
BFD Destination unreachable	Number of times the destination IP address for a BFD neighbor was unreachable while the ACOS was attempting to transmit a BFD packet to the neighbor.

Field	Description
BFD Other error	Number of BFD errors not counted in any of the fields above.

show bootimage

Description Display the software images stored on the ACOS Device.

Syntax

```
show bootimage
```

Mode All

Example The following command shows the software images on an A10 Thunder Series 4430 device:

```
ACOS#show bootimage
(* = Default)
                            Version
-----------------------------------------------
Hard Disk primary           4.0.0.485
Hard Disk secondary         2.7.2-P2-SP6.1 (*)
Compact Flash primary       2.7.2.191 (*)
Compact Flash secondary     2.7.2.191
```

The asterisk (*) indicates the default image for each boot device (hard disk and compact flash). The default image is the one that the ACOS Device will try to use first, if trying to boot from that boot device. (The order in which ACOS tries to use the image areas is controlled by the bootimage command.)

show bpdu-fwd-group

Description Display the configured Bridge Protocol Data Units (BPDU) forwarding groups.

Syntax

```
show bpdu-fwd-group [number]
```

Specify a BPDU forwarding group *number* to view the configuration of the specified BPDU forwarding group. If you omit this option, all configured BPDU forwarding groups are shown.

Mode All

Example The following command shows all configured BPDU forwarding groups:

```
ACOS#show bpdu-fwd-group
BPDU forward Group 1 members:  ethernet 1 to 3
BPDU forward Group 2 members:  ethernet 9 to 12
```

show bridge-vlan-group

Description Display information for a bridge VLAN group.

Syntax `show bridge-vlan-group [group-id]`

Mode All

show bw-list

Description Show black/white list information.

Syntax `show bw-list [name [detail | ipaddr]]`

Parameter	Description
name	Name of a black/white list.
detail	Displays the IP addresses contained in a black/white list.
ipaddr	IP address within the black/white list.

Default N/A

Mode Config

Example The following command shows all the black/white lists on an ACOS Device:

```
ACOS#show bw-list
```

```
Name            Url                                  Size(Byte)
Date
-------------------------------------------------------------------
--------------
bw1             tftp://192.168.1.143/bwl.txt          106
Jan/22 12:48:01
bw2             tftp://192.168.1.143/bw2.txt          211
Jan/23 10:02:44
bw3             tftp://192.168.1.143/bw3.txt          192
Feb/11 08:02:01
bw4             Local                                  82
Dec/12 21:01:05
Total: 4
```

Example The following command shows the IP addresses in black/white list “test”:

```
ACOS#show bw-list test detail
Name:                test
URL:                 tftp://192.168.20.143/bwl_test.txt
Size:                226        bytes
Date:                May/11 12:04:00
Update period:       120 seconds
Update times:        2

Content
-------------------------------------------------------------------
----------------
1.1.1.0 #13
1.1.1.1 #13
1.1.1.2 #13
1.1.1.3 #13
1.1.1.4 #13
9.9.99.9 9
1.2.3.4/32 31
4.3.2.1/24 4
10.1.2.1/32 1
10.1.2.2/32 2
10.1.2.3/32 3
10.1.2.4/32 4
```

```
10.3.2.1/32 3
10.3.2.2/32 4
10.5.2.1/32 5
10.5.2.2/32 6
128.0.0.0/1 11
```

show class-list

Description Display information for class lists.

Syntax **show class-list** [*name* [*ipaddr*]]

Replace *name* with the class list name or *ipaddr* with an IP address in the class list. If neither option is specified, the list of configured class lists is displayed instead.

Mode All

Usage For Aho-Corasick (AC) class lists, enter the `write memory` command immediately before entering **show class-list**.

Example The following command displays the class-list files on the ACOS Device device:

```
ACOS# show class-list
Name       Type     IP        Subnet    DNS       String    Location
CL1       [ipv4]    4         0         0         0         config
CL2       [ipv4]    0         1         0         0         config
Total: 2
```

The following table describes the fields in the command output.

Field	Description
Name	Name of the class list.
Type	AC, IPv4, or IPv6.
IP	Number of host IP addresses in the class list.
Subnet	Number of subnets in the class list.
DNS	Number of DNS servers in the class list.

Field	Description
String	Number of strings in the class list.
Location	Indicates whether the class list is in the startup-config or in a standalone file: config – Class list is located in the startup-config. file – Class list is located in a standalone file.
Total	Total number of class lists on the ACOS Device device.

The following command shows details for a class list, including the hit count:

```
ACOS# show class-list test
Name:                CL2
Total single IP:     0
Total IP subnet:     1
Content:
    0.0.0.0/0 lid 31
```

The following commands show the closest matching entries for specific IP addresses in class list “test”:

```
AOCS# show class-list CL1 1.1.1.1
    1.1.1.1/32 glid 1
ACOS# show class-list CL1 2.2.2.2
    0.0.0.0/0 lid 31
```

Class list CL1 contains an entry for 1.1.1.1, so that entry is shown. However, since class list CL2 does not contain an entry for 1.1.1.1 but does contain a wildcard entry (0.0.0.0), the wildcard entry is shown.

show clns

Description Show Connectionless Network Service (CLNS) information.

Syntax

```
show clns [tag] [is-neighbors | neighbors]
[
 ethernet num |
 lif num |
 loopback num |
 management |
 trunk num |
```

```
 tunnel num |
 ve num
]
[detail]]
```

The following table describes the fields in the command output.

Parameter	Description
is-neighbors	Displays IS neighbor adjacencies.
neighbors	Displays CLNS neighbor adjacencies.
ethernet *num*	Display adjacency information for the specified ethernet interface.
lif *num*	Display adjacency information for the specified logical interface.
loopback *num*	Display adjacency information for the specified loopback interface.
management	Display adjacency information for the management interface.
trunk *num*	Display adjacency information for the specified trunk.
tunnel *num*	Display adjacency information for the specified tunnel.
ve *num*	Display adjacency information for the specified virtual interface.
detail	Displays detailed information.

Mode All

Example The **show clns neighbors** command displays IS-IS helper information when ACOS is in helper mode for a particular IS-IS neighbor. Here is an example:

```
ACOS#show clns neighbors
Area ax1:
System Id      Interface   SNPA                State  Holdtime
 Type Protocol
```

```
0000.0000.0004 ethernet 10 78fe.3d32.880a     * Up      99
 L2    M-ISIS
```

The asterisk (*) character in the output indicates that IS-IS is in helper mode for the neighbor.

show clock

Description Display the time, timezone, and date.

Syntax

```
show clock [detail]
```

Parameter	Description
detail	Shows the clock source, which can be one of the following: Time source is NTP Time source is hardware calendar

Mode All

Example The following command shows clock information for an ACOS Device:

```
ACOS#show clock detail
20:27:16 Europe/Dublin Sat Apr 28 2007
Time source is NTP
```

Example If a dot appears in front of the time, the ACOS Device has been configured to use NTP but NTP is not synchronized. The clock was in sync, but has since lost contact with all configured NTP servers.

```
ACOS#show clock
.20:27:16 Europe/Dublin Sat Apr 28 2007
```

Example If an asterisk appears in front of the time, the clock is not in sync or has never been set.

```
ACOS#show clock
*20:27:16 Europe/Dublin Sat Apr 28 2007
```

show config

Description This command displays the entire running configuration

Syntax

```
show config
```

Default N/A

Mode Global

Usage Use this command to display the entire running configuration for the ACOS Device, or for the particular partition which you are viewing.

Related Commands:

- show running-config

show config-block

Description This command displays the current configurations being made in either block-merge or block-replace mode.

Syntax

```
show config-block
```

Default N/A

Mode Block-merge or Block-replace configuration mode

Usage Use this command to display the uncommitted configurations you have made in either block-merge or block-replace mode. These commands are not a part of the running configuration, but they will be implemented upon ending block-merge or block-replace mode.

show config-sync

Description Show the status of config-sync for all partitions in a VRRP-A environment.

Synchronizing configurations is done using the configure sync command.

Syntax `show config-sync [all-partitions] [detail]`

Parameter	Description
`all-partitions`	View the config-sync information in all partitions. This option is only available from the shared partition, meaning that in the shared partition you can view the sync status for all partitions, but from inside a private partition, only the sync status of that partition is available.
`detail`	By default, the output only shows the current sync status for the running-config and startup-config; whether it is sync'ed to the peer, or sync'ed from the peer. The `detail` option shows the following four options, and will show the last time a "sync from peer" option was changed from a "sync to peer" configuration, or vice-versa. • Sync status for the running-config to the peer • Sync status for the startup-config to the peer • Sync status for the running-config from the peer • Sync status for the startup-config from the peer

Mode All

Example For various examples, "Viewing VRRP-A Information" in the *Configuring VRRP-A High Availability* guide.

show configure sync log

Description Displays the status and detail log of configuration synchronization activities between the local device and its peer, including initiation, progress, file transfers, and completion events.

Syntax `show configure sync log`

Example The following example shows the detail configuration synchronization activities between the local device and its peer:

Mode All

```
ACOS#show configure sync log
Jul 23 2025 22:21:55 Info CONFIG SYNC(WHOLE): completely
Jul 23 2025 22:21:55 Info CONFIG SYNC: set partitions inactive
: (!) (Done)
Jul 23 2025 22:21:52 Info CONFIG SYNC: Sync startup-config
completely
Jul 23 2025 22:21:10 Info CONFIG SYNC: Sync startup-config
Jul 23 2025 22:21:10 Info CONFIG SYNC(WHOLE): STARTUP-CONFIG
Jul 23 2025 22:20:43 Info CONFIG SYNC: Sync running-config
without reload
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files directory [SSLiOut] [pri_default]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_xsd]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_wsdl]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_waf]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_rpz]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_lw-4o6]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_key]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_ip-map-list]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_hm]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_gslb]
Jul 23 2025 22:20:43 Info CONFIG SYNC : copy/overwrite data
files [SSLiOut][g_dnssec]
```

show context

Description View the configuration for the sub-module in which the command is run.

For example, if you are configuring a virtual port under a virtual server, the **show context** command displays only the portion of the configuration within the context of the virtual port configuration.

Unlike other **show** commands, the **show context** command is only available in Global configuration mode, or any additional sub-mode. For example, if you are configuring a port under an SLB server, this command shows only the configuration related to the port.

Syntax

```
show context
```

Mode Global configuration mode or further sub-modes

Example The following example shows the portion of the configuration related to BGP AS 1:

```
ACOS(config)#router bgp 1
ACOS(config-bgp:1)#show context
!Section configuration: 216 bytes
!
router bgp 1
  network 2.2.2.2/32
  neighbor a peer-group
  neighbor 3.3.3.3 remote-as 1
  address-family ipv6
    bgp dampening 3 3 3 3
    neighbor a activate
    neighbor a capability orf prefix-list send
```

Example The following example first shows the portion of the running-config related to server s1, then only the portion related to port 80:

```
ACOS(config-bgp:1-ipv6)#slb server s1
ACOS(config-real server)#show context
!Section configuration: 104 bytes
!
slb server s1 1.1.1.1
```

```
  port 80 tcp
    weight 2
    conn-limit 2
    conn-resume 1
  port 81 tcp
ACOS(config-real server)#port 80 tcp
ACOS(config-real server-node port)#show context
!Section configuration: 64 bytes
!
port 80 tcp
    weight 2
    conn-limit 2
    conn-resume 1
```

show core

Description Display core dump statistics.

Syntax

```
show core [process]
```

The **process** parameter shows core dump statistics for processes on the ACOS Device. Without this option, system core dump statistics are shown instead.

Mode Privileged EXEC level and configuration levels.

Example The following command shows system core dump statistics:

```
ACOS#show core
The LB process has reloaded 1 time.
The LB process has crashed 0 time.
The LB process has been up for 2755 seconds.
```

show core-slots

Description Displays core slots dump statistics.

Syntax

```
show core-slots
```

Mode Privileged EXEC level and configuration levels.

Example The following command shows system core slot dump statistics:

```
ACOS#show core-slots

Processing-Unit : 1
The LB process has reloaded 1 time.
The LB process has crashed 1 time.
The LB process has been up for 90043 seconds.

Processing-Unit : 2
The LB process has reloaded 2 time.
The LB process has crashed 1 time.
The LB process has been up for 90049 seconds.
ACOS#
```

show counters-all slb hm-dplane

Description Shows SLB counters information of the data plane health monitoring.

Syntax

```
show counters-all slb hm-dplane [entry]
```

Mode All

Example

```
ACOS(config)#show counters-all slb hm-dplane entry

show counters-all slb hm-dplane entry
-------------------------------------
Current Entry Count
  1
Total Entry Created
  4
Total Entry Inserted
  4
Total Entry Ready To Free
  0
Total Entry Freed
  2
Entry Creation Failure
  0
```

```
Entry Creation Out of Memory
  0
Entry Insert Failed
  0
Total TCP errors in health check sent out
  0
Error creating Smart NAT Instance
  0
Error obtaining Smart NAT source port
  0
Error allocating L4 session for HM
  0
Error in initiating TCP connection for HM
  0
TCP connection sent for HM
  27533
Entry Deleted
  2
Error in creating HM internal VIP
  0
Total HTTP received response with match response code
  0
Total HTTP received response with match 200 response code
  27564
Total HTTP received response with match 200 response code
  0
Total HTTP received response with wrong response code
  0
Error no HM entry found
  0
Error SSL cert name mismatch
  0
Error SSL server SYN timeout
  0
Error SSL server SYN timeout
  0
L7 session process TCP estab. failed
  0
```

```
L7 session process TCP data failed
  0
Error http2 version mismatch
  0
```

show counters acos-events statistics

Description Displays the statistic of the acos-event counters.

Syntax

```
show counters acos-events statistics
```

Parameter	Description
`show counters acos-events statistics`	Displays the ACOS events statistics. Following is a list of counters that are shown along with reason for each: • **Messages sent, to Remote** - Incremented when a log is sent to a remote log server • **Messages sent, to LogDB** - Incremented when a log is sent to the local database, which is used for the GUI. • **Messages Dropped, format not defined** - Incremented when the format for a given log message that is enabled by the selector and collector group is not defined in schema. • **Messages Dropped, malloc failure** - Incremented when we could not get a buffer to send to the log-server. • **Messages Dropped, no active template** - Should be incremented when there is an issue with the active template to send a log. • **Messages Dropped, selector does not enable msg** - Incremented when a log message is not enabled in the selector.

Parameter	Description
	• **Message Dropped, invalid length** - Incremented when the length of the message is longer than the length supported by the transport (usually UDP). • **Messages Dropped, msg crafting failed** - Incremented when there is a problem trying to craft the log message. For example, there is an issue with the schema definition or length issue. • **Messages Dropped, local log ratelimited** - Incremented when we hit rate limit for local logs like `show logs` and `show varlog`, to not overwhelm the Contorl CPU. • **Messages Dropped, send failed** - Incremented when there is a failure while sending the log to a remote server. • **Messages Dropped, no active member in collector grp** - Incremented when there are no log-servers in a collector-group or none of the configured log-servers are reachable when a log is sent to a template that is using the collector-group. • **Messages Dropped, Route lookup failed** - Incremented when a route to the destination log-server is not found. • **Messages Dropped, unexpected error** - Incremented when an unexpected error happens, sometimes due to configuration transition (usually while it is being changed), other times some internal issue.

Example The following command displays the statistic of acos-even counters.

```
vThunder#show counters acos-events statistics

show counters acos-events statistics
-------------------------------------
Messages sent, to Remote
  0
Messages sent, to LogDB
  0
Messages Dropped, format not defined
  0
Messages Dropped, malloc failure
  0
Messages Dropped, no active template
  0
Messages Dropped, selector does not enable msg
  0
Messages Dropped, invalid length
  0
Messages Dropped, msg crafting failed
  0
Messages Dropped, local log ratelimited
  0
Messages Dropped, send failed
  0
Messages Dropped, no active member in collector grp
  0
Messages Dropped, Route lookup failed
  0
Messages Dropped, unexpected error
  0
Parameterized log sent to HC
  0
Parameterized log send to HC failed
  0
Parameterized log AVRO encoding failed
  0
```

show counters acos-events collector-group

Description Displays the collector group for acos-event counters.

Syntax

```
show counters acos-events collector-group
```

Parameter	Description
`show counters acos-events collector-group`	Displays the counters for each collector-group level. Following is a list of counters that are shown along with reason for each: • **Number of log messages sent** - Incremented when a message is sent to all the log severs in a collector-group. • **Number of rate limited log messages** - Incremented when the rate-limit of a collector group is hit.

Example The following command displays the collector group for acos even counters.

```
vThunder#show counters acos-events collector-group cg

show counters acos-events collector-group cg
--------------------------------------
Number of log messages sent
  0
Number of rate limited log messages
  0
```

show counters drop | error

Description Display counters for errors and drops. Use tags to display specific information for troubleshooting.

Syntax

```
show counters
```

Parameter	Description
counters error	Displays error counters
counters error alert	Display alert error counters.
counters error critical	Display critical error counters
counters error warning	Display warning error counters
counters error out-of-res	Display errors due to resource exhaustion
counters drop	Display drop counters
counters drop alert	Display alert drop counters
counters drop critical	Display critical drop counters
counters drop warning	Display warning drop counters
counters drop out-of-res	Display drops due to resource exhaustion

Default NA

Mode All

Example This displays the counter drops.

```
ACOS(config)#show counters drop
/slb/switch
************************************
L2 Default Vlan FWD Drop 40
Prot Down Drop 2
Unknown Prot Drop 6
ARP PKT dropped due to virtual IP not found 151
```

show counters system ip-threat-list

Description Display the IP Threat List counters. For more information on IP Threat list, refer to the *Firewall Configuration* guide .

Syntax

```
show counters system ip-threat-list
```

Default NA

Mode Configuration Mode

NOTE: The Packet Hit Count in SPE is updated for every 4096 packets per entry or upon removal of an entry from the SPE. All the SPE related counters are incremented on SPE supported platforms only.

Example

```
ACOS(config)# show counters system ip-threat-list
Packet Hit Count in SW
5
Packet Hit Count in SPE
  0
Entries Added in SW
   6
Entries Removed from SW                                    0
Entries Added in SPE
   0
Entries Removed from SPE                                   0
Out of memory Error
   0
Out of SPE Entries Error
  0
```

The following table describes the fields in the command output:

Parameter	Description
Packet Hit Count in SW	The total number of packets that hit the entries in the threat list
Packet Hit Count in SPE	The total number of packets that hit the entries in the Security Policy Engine (SPE)
Entries Added in SW	The total number of entries added to the threat list
Entries Removed from SW	The total number of entries removed from the threat list
Entries Added	The total number of entries added to SPE

Parameter	Description
in SPE	
Entries Removed from SPE	The total number of entries removed from SPE
Out of memory Error	Displays the following error: *Unable to create an entry in the IP threat list due to memory exhaustion*
Out of SPE Entries Error	Displays the following error: *Unable to add entries to SPE due to SPE resource limit or exhaustion*

show counters system session

Description Display the system session counters.

Syntax

```
show counters system session
```

Default NA

Mode Configuration Mode

Example The following command shows the system session counters:

```
show counters system session
-------------------------------------
Total L4 Count                        0
Conn Count                            28
Conn Freed                            28
Total L4 Packet Count                 0
Total L7 Packet Count                 0
Total L4 Conn Proxy Count             0
Total L7 Conn                         0
Total TCP Conn                        0
Curr Free Conn                  2039787
TCP Established                       0
TCP Half Open                         0
TCP Half Closed                       0
UDP Count                             0
```

```
IP Count                                0
Non TCP/UDP IP sessions                 0
Reverse NAT TCP                         0
Reverse NAT UDP                         0
TCP SYN Half Open                       0
Conn SMP Alloc                          7
Conn SMP Free                           0
Conn SMP Aged                           0
Curr SSL Count                          0
Total SSL Count                         0
Current SSL Server Count                0
Total SSL Server Count                  0
Total SSL Client Reuse                  0
Total SSL Server Reuse                  0
Total IP Nat Conn                       0
Totl L2/L3 Connections                  0
Conn Type 0 Available             3538944
Conn Type 1 Available             1933307
Conn Type 2 Available             917502
Conn Type 3 Available             450559
Conn Type 4 Available             221184
Conn SMP Type 0 Available         3538944
Conn SMP Type 1 Available         1769472
Conn SMP Type 2 Available         884736
Conn SMP Type 3 Available         450552
Conn SMP Type 4 Available         221184
SCTP Half Open                          0
SCTP Established                        0
Conn APP SMP Alloc                      0
Diameter Conn Count                     0
Diameter Conn Freed                     0
Total Firewall Conn                     0
Total Local Conn                        0
Total Curr Conn                         0
client ssl fatal alert                  0
client ssl fin rst                      0
FP Session FIN/RST                      0
server ssl fatal alert                  0
server ssl fin rst                      0
client template internal error          0
```

```
client template unknown error          0
server template int error              0
server template unknown error          0
Diameter Concurrent User-Sessions      0
Total SSL Client Session Ticket Reuse 0
Total SSL Server Session Ticket Reuse 0
Total clientside early data connections 0
Total serverside early data connections 0
Total clientside failed early data connections        0
Total serverside failed early data connections        0
Total Logging Conn                     0
GTP-C Established                      0
GTP-C Half Open                        0
GTP-U Count                            0
GTP-C Echo Count                       0
GTP-U Echo Count                       0
GTP Current Available Conn        203978
GTP cumulative Conn Count              0
GTP cumulative Conn Freed              0
Blacklist Sessions                     0
Blacklist Session Created             13
Blacklist Session Freed               13
```

show cpu

Description Displays the CPU usage.

Syntax

```
show cpu [history | overall]
```

Parameter	Description
history	Shows control CPU and data CPU usage information.
overall	Shows overall CPU utilization.

Mode Privileged EXEC level and configuration levels

If you enter the **show cpu** command from within an L3V partition, the command shows utilization for only that partition.

Example The following command shows overall CPU utilization:

```
ACOS(config)#show cpu overall
Time: May-12-2023, 12:47
                  1Sec     5Sec     10Sec    30Sec     60Sec
-------------------------------------------------------------
Control1          25%      26%      25%      26%       27%
Data1             0%       0%       0%       0%        0%
Data2             0%       0%       0%       0%        0%
I/O1              0%       0%       0%       0%        0%
```

The following table describes the fields in the command output.

Field	Description
Time	System time when the statistics were gathered.
Control *n*	Control CPU.
Data*n*	Data CPU. The number of data CPUs depends on the ACOS model.
I/O*n*	IO CPU usage. I/O fields are displayed on non-FTA platforms only.
1Sec - 60sec	Time intervals at which statistics are collected.

Example

The following command output displays CPU utilization rates plotted over the last 60 seconds. The x-axis represents the time elapsed and the y-axis represents the CPU utilization rate. Asterisks appear along the bottom of the output to illustrate the CPU utilization rates over time. The figure below only shows the usage for the Control CPU. The usage for the Control CPU and Data CPU are displayed in separate figures. The CLI command prints 1 asterisk for every 10 percent utilization. This means no asterisk will be printed if the CPU usage is from 0-4; one asterisk will be printed if the CPU usage is 5-14; two asterisks will be printed if the CPU usage is 15-24; and so on.

```
ACOS(config)#show cpu history
Time: 12:33:00 IST Fri May 12 2023
   22222333332322222222222222222222232322233333332222223234
3
```

```
   6787951222817557379755558487484678809736791000002975585061
4
100
 90
 80
 70
 60
 50
 40     *                                                     *
 30**************** ******** ** *
****************************

20************************************************************
 1
0************************************************************

  0....0....1....1....2....2....3....3....4....4....5....5....
        5    0    5    0    5    0    5    0    5    0    5
     Control CPU1:   CPU% per second (last 60 seconds)
   3222222222222222222222232222222222222222222222222222222
2

  0577657769849776765876660919877658676659857567957676659886
100
 90
 80
 70
 60
 50
 40
 30***********
*********************************************
 2
0************************************************************
 1
0************************************************************
   0....0....1....1....2....2....3....3....4....4....5....
5....
        5    0    5    0    5    0    5    0    5    0    5
       Control CPU1:   CPU% per minute (last 60 minutes)
```

```
   22222222222222222222222222222222222222222222222222222222222222
2222222222222
   77777777777777777777777777777777676777777777777777777777777777
7677777777777
100
 90
 80
 70
 60
 50
 40

3
0************************************************************
***********
 2
0************************************************************
***********
 1
0************************************************************
***********
   0....0....1....1....2....2....3....3....4....4....5....5...
.6....6....7.
        5    0    5    0    5    0    5    0    5    0    5
0    5    0
     Control CPU1:   CPU% per hour (last 72 hours)
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....0....1....1....2....2....3....3....4....4....5....
5....
        5    0    5    0    5    0    5    0    5    0    5
     Data CPU1:   CPU% per second (last 60 seconds)
```

show debug

Description This command applies to debug output. It is recommended to use the axDebug subsystem commands instead of the debug commands.

Example The show debug output is as follows:

```
ACOS(7650)#show debug
debug packet is on
debug http-proxy (level 1) is on
debug http2 (level 1) is on
debug ssl is on
```

Related Commands:

- show axdebug file
- show axdebug filter
- show axdebug status

show disk

Description Display status information for the ACOS Device hard disks.

Syntax

```
show disk
```

Mode Privileged EXEC level and configuration levels

Example The following command shows hard disk information for an A10 Thunder Series 4430 device:

NOTE: The output on your device may differ slightly from the one shown below.

```
ACOS#show disk
Total(MB)  Used       Free       Usage
-----------------------------------------
  95393      11301      84091      11.8%

  Device   Primary Disk        Secondary Disk
-----------------------------------------------
```

```
md0       Active
md1       Active
```

The following table describes the fields in the command output.

Field	Description
Total(MB)	Total amount of data the hard disk can hold. **NOTE:** The hard disk statistics apply to a single disk. This is true even if your ACOS Device contains two disks. In systems with two disks, the second disk is a hot standby for the primary disk and is not counted separately in the statistics.
Used	Number of MB used.
Free	Number of MB free.
Usage	Percentage of the disk that is in use.
Device	Virtual partition on the disk: • md0 – The boot partition • md1 – The A10 data partition
Primary Disk	Status of the left hard disk in the redundant pair: • Active – The disk is operating normally. • Inactive – The disk has failed and must be replaced. Contact technical support. • Synchronizing – The disk has just been installed and is synchronizing itself with the other disk.
Secondary Disk	Status of the right hard disk in the redundant pair.

show dns cache

Description Display DNS caching information created by load balancing.

Syntax

```
show dns cache [ client | entry options | global options |
rate | statistics | template <template-name> options |
virtual-server <virtual_server_name> <virtual_port> <port_
type> options ]
```

Parameter	Description
client	Displays DNS client statistics.
entry *options*	Displays DNS cache entries from the system-wide cache. Filters can be applied.
global *options*	Displays global DNS cache entries. Filters can be applied.
rate	Displays DNS cache rates.
statistics	Displays DNS caching statistics.
template *<template_name> options*	Displays DNS entries from the shared cache of

Parameter	Description
	the specified DNS template. Filters can be applied.
virtual-server *<virtual_server_name> <virtual_port> <port_type> options*	Displays DNS cache entries for the specified virtual server, vPort, and port type. Filters can be applied.

The following *options* are available for filtering DNS cache entries:

Parameter	Description
all-entries	Displays all the DNS cache entries without limiting the display to the default value of 10,000. If configured, the display of cache entries may take a longer time if the number of entries is large.

Parameter	Description
dns-class *suboptions*	Displays cache entries matching the specified DNS class. The following *suboptions* are available: • **IN** – INTERNET class • **CH** – CHAOS class • **HS** – HESIOD class • **NONE** – NONE class • **ANY** – ANY class • *num* – Custom class value (1-65535)
dns-type *suboptions*	Displays cache entries matching the specified DNS record type. The following *suboptions* are available: • **A** – Address type • **AAAA** – IPv6 Address type

Parameter	Description
	• **CNAME** – Canonical name type • **MX** – Mail exchange type • **NS** – Name server type • **SRV** – Service locator • **PTR** – PTR resource type • **SOA** – Start of authority type • **TXT** – Text type • **ANY** – All cached type • *num* – Custom type value (1-65535)
domain *suboptions*	Displays DNS cache entries for a specific domain. The following *suboptions* are available: • **dns-domain-name** – Domain name • **fqdn-domain** –

Parameter	Description
	Fully qualified domain name
brief *suboptions*	Displays the DNS response resource records of the cache entry in brief. It displays only the answer section. The following *suboptions* are available: • **max-rdata-size** – Specifies the maximum rdata size for each record. The following options are available: ◦ **<1 to 8192>** – Specifies the maximum rdata size to be displayed for each record. ◦ **all** – Displays full

Parameter	Description
	content of rdata for each record; maximum limit is 8192 characters. • **max-record-num** – Specifies the number of maximum records to be displayed for each section of the cache entry. The following options are available: ○ **<1-1024>** – Specify the number of records to be displayed for each section of cache entry. ○ **all** – Displays all the records for each section of cache entry;

Parameter	Description
	maximum limit is 1024 records.
detail *suboptions*	Displays the DNS response resource records of the cache entry in detail. It displays the answer section, authority section and additional section. • **detail** – Displays the DNS response resource records of the cache entry in detail. It displays the answer section, authority section and additional section. The following *sub-options* are available: ◦ **max-rdata-size** –

Parameter	Description
	Specify the maximum rdata size for each record. The following options are available: ○ **<1 to 8192>** – Specify the maximum rdata size to be displayed for each record. ○ **all** – Displays full content of rdata for each record; maximum limit is 8192 characters. ○ **max-record-num** – Specify

Parameter	Description
	the number of maximum records to be displayed for each section of the cache entry. The following options are available: ○ **<1-1024>** – Specify the number of records to be displayed for each section of cache entry. ○ **all** – Displays all the records for each section of cache entry; maximum

Parameter	Description
	limit is 1024 records.

Mode All

Usage Use this command to display DNS cache entries system-wide, per DNS template, or per virtual server/port. The supported filters may be used individually or in combination (multiple-choice filtering).

- You can view all or selective entries using filters.
- You can view DNS statistics and client counters.

NOTE: If the specified virtual-server, virtual port, or DNS template is invalid or does not exist, the system does not display any output.

Example The following command shows information about the clients that have interacted with the DNS cache:

```
ACOS(config)# show dns cache client
Client class list statistics:
    F = Flag (C-Connection, R-Request), Rate(per sec), Over-RL
= Over rate limit
Domain                    Destination           F Rate
Over-RL   lock       lock-time
------------------------+--------------------+-+---------+--
-------+----------+----------
youtube.com               10.214.6.100:53       C 0         2
       0          0  <<- limit_stat of per vport
youtube.com               *                     C 0         6
       0          0  <<- limit_stat of global-dns-cache
Total: 2
```

The '*' symbol in the **Destination** field in the above output indicates that the traffic is targeting the entire partition for load balancing rather than individual vports within the partition.

Example

The following command shows DNS caching entry detail. A, AAAA, TXT, CNAME, MX and NS records are displayed in string format, whereas all other records are shown in hex values.

```
ACOS(config)# show dns cache entry detail
N = Negative, S = DNSSEC, T = Type, C = Class, Qlen = Query
length, Rlen = Response length
 an = Answer RRs number, ns = Authority RRs number, ar =
Additional RRs number
Domain                              N   S   T   C   Qlen  Rlen
an   ns   ar
T    C  TTL  RDLENGTH RDATA
------------------------------------+---+---+---+---+-----+----
-+----+----+----------------
cache usage: 0.00%
cache hit ratio: 4.65%
tcp:dns-udp:53
------------------------------------------------------------------
------------------------
loc.santest.xyz                     0   0   29  1   33    49
1    0    1
[Answer section]
29   IN 86400    16   00541513881b16a865bb507800989a68
[Additional section]
OPT                  EDNS: version: 0, flags:, udp: 1232
------------------------------------------------------------------
------------------------
uri.santest.xyz                     0   0   256 1   33    64
1    0    1
[Answer section]
256  IN 86400    31
000a0014687474703a2f2f73616e746573742e78797a2f7265736f75726365
[Additional section]
OPT                  EDNS: version: 0, flags:, udp: 1232
------------------------------------------------------------------
------------------------
hostmaster.santest.xyz              0   0   16  1   40    79
1    0    1
[Answer section]
TXT  IN 86400    46   "Responsible person for santest.xyz"
```

```
[Additional section]
OPT                    EDNS: version: 0, flags:, udp: 1232
------------------------------------------------------------------
-------------------------
afs.santest.xyz                      0    0    18   1    33     59
1     0     1
[Answer section]
18    IN 86400     26
00010a6166732d7365727665720773616e746573740378797a00
[Additional section]
OPT                    EDNS: version: 0, flags:, udp: 1232
------------------------------------------------------------------
-------------------------
santest.xyz                          0    0    17   1    29     76
1     0     1
[Answer section]
17    IN 86400     43
0561646d696e0773616e746573740378797a000a686f73746d617374657207
7
3616e746573740378797a00
[Additional section]
OPT                    EDNS: version: 0, flags:, udp: 1232
------------------------------------------------------------------
-------------------------
santest.xyz                          0    0    1    1    29     37
1     0     1
[Answer section]
A     IN 86400     4     192.168.1.10
[Additional section]
OPT                    EDNS: version: 0, flags:, udp: 1232
------------------------------------------------------------------
-------------------------
host1.santest.xyz                    0    0    13   1    35     49
1     0     1
[Answer section]
13    IN 86400     16    09496e74656c20783836054c696e7578
[Additional section]
OPT                    EDNS: version: 0, flags:, udp: 1232
Total: 7
```

Example The following command shows the cached DNS entries for the specified template:

```
ACOS(config)# show dns cache template test
            N = Negative, S = DNSSEC, T = Type, C = Class, W =
weight
                          Qlen = Query length, Rlen = Response
length
Domain                                N    S  T    C    Qlen Rlen
TTL     Age     W  Hit
-----------------------------------+---+---+---+---+-----+----
-+-------+-------+--+-------
cache usage: 0.00%
cache hit ratio: 23.08%
Template: test
www.example.com                     0    0  1    1    33   37
500     0       1  0
www.google.com                      0    0  1    1    32   37
500     0       1  0
Total: 2
```

Example The following command shows the cached DNS entries for the specified virtual server, vPort, and port type:

```
ACOS(config)# show dns cache virtual-server vs3 53 dns-tcp
             N = Negative, S = DNSSEC, T = Type, C = Class, W
= weight
                            Qlen = Query length, Rlen =
Response length
Domain                                N    S    T    C    Qlen  Rlen
 TTL     Age      W  Hit
-----------------------------------+---+---+---+---+-----+----
-+-------+-------+--+-------
cache usage: 0.00%
cache hit ratio: 0.00%
Total: 0
```

Example The following command shows DNS caching statistics:

```
ACOS(config)# show dns cache statistics
Total allocated: 620404
```

```
Total freed: 310211
Total query: 57333516
Total server response: 680521
Total cache hit: 56652978
Query not passed: 0
Response not passed: 2
Query exceed cache size: 0
Response exceed cache size: 0
Response answer not passed: 0
Query encoded: 0
Response encoded: 0
Query with multiple questions: 0
Response with multiple questions: 0
Response with multiple answers: 0
Response with short TTL: 0
Total aged out: 310211
Total aged for lower weight: 0
Total stats log sent: 0
Response truncated: 0
******The following counters are global to system and not per
partition*****
Current allocate: 310193
Current data allocate: 0
```

NOTE: When a partition contains more than 100,000 entries, the global overflow LID receives DNS requests. By default, this LID disables the DNS cache. Depending on the platform, increase the parameter "pbslb-entry-count" in SLB resource usage to support up to 32 million entries.

The following table describes the fields in the command output.

Field	Description
Total Allocated	Total number of allocated for cache entries.
Total Freed	Total number of released for cache entries.
Total Query	Total number of DNS queries received by the ACOS.

Field	Description
Total Server Response	Total number of responses form DNS servers received by the ACOS.
Total Cache Hit	Total number of times the ACOS was able to use a cached reply in response to a query.
Query Not Passed	Number of queries that were not passed a packet sanity check.
Response Not Passed	Number of responses that were not passed a packet sanity check.
Query Exceed Cache Size	Number of queries that were bypassed from caching process because their size exceeds the configured maximum cache size.
Response Exceed Cache Size	Number of responses that were not cached because their size exceeds the configured maximum cache size.
Response Answer Not Passed	Number of responses that were not cached because no type matched answer records were available.
Query Encoded	Number of queries that were bypassed from caching process because the domain name in the question record contained a compressed label and considered as malformed.
Response Encoded	Number of responses that were not cached because the domain name in the question record contained a compressed label and considered as malformed.
Query With Multiple Questions	Number of queries that were bypassed from caching process because they contained multiple question records. ACOS only supports one question record.
Response With Multiple	Number of responses that were not cached because they contained multiple question records. ACOS only supports one question record.

Field	Description
Questions	
Response With Multiple Answers	Number of responses that were not cached because they contained more than one answer, when `single-answer` caching policy was enabled. This behavior only applies to DNS “IN” class and “A” or “AAAA” types.
Response with Short TTL	Number of responses that were not cached because they had short record time to live (TTL), when `ttl-threshold` caching policy was enabled. This behavior only applies to DNS “IN” class and “A” or “AAAA” types.
Total Aged Out	Total number of DNS cache entries that have aged out.
Total Aged for Lower Weight	Number of cache entries that were aged out when the cache occupancy reached a specific percentage and the weight value was below the threshold.
Total Stats Log Sent	Total number of logs sent after the cache hit occurs. This feature is applicable only to VIP DNS Cache and requires the **`dns-log-enable period`** option to be enabled in the DNS template that is bound to the DNS VIP. This can send the logs either locally, or to both locally and to the syslog server, depending on the configuration.
Response truncated	Number of responses that were truncated because their cache size exceeds the client's maximum UDP payload size.
Current Allocate	Current allocated cache entries.
Current Data Allocate	Current data allocation.

Related Commands:

slb template dns

show dns-cache

Description Display DNS caching information created by the system.

Syntax

```
show dns-cache
```

Mode All

Example The following example shows example output for this command.

```
ACOS(config)# show dns-cache
Record Name            A/CNAME Record          DNS Server
     TTL
www.example.com        210.149.5.50           10.255.237.22
     17

Total: 1
```

Related Commands:

slb template dynamic-service

show dns persistent-cache

Description Displays persistent cache statistics and entries.

Syntax

```
show dns persistent-cache
[entry | statistics]
```

Option	Description
entry	Shows DNS persistent cache entries.
statistics	Shows DNS persistent cache statistics.

Mode All

Usage One of the options must be specified.

Example The following example shows persistent cache entries:

```
ACOS# show dns persistent-cache entry
                              S = DNSSEC, T = Type, C = Class
                             Qlen = Query length, Rlen =
Response length
Domain                                  S     T    C    Qlen   Rlen
TTL
-----------------------------------+---+---+-----+-----+------
-+-------
 test.dnsrr.com                         0    2    1    32     90
300
 www.test.dnsrr.com                     0    1    1    36     98
300
 ns3.test.dnsrr.com                     0    1    1    36     26
300
Total: 3
```

Example The following example shows persistent cache statistics:

```
ACOS# show dns persistent-cache statistics
                        Total
-----------------------------------------------
Total persistent cache 3
Total saved            3
Total deleted          0
Database Busy          0
Database Error         0
```

show dns response-rate-limiting entries

Description Display DNS response rate limiting entries.

Syntax

```
show dns response-rate-limiting entries {fqdn | full-width |
ipv4 | ipv6}
```

Parameter	Description
fqdn	Filter by requested FQDN.
full-width	Display full ipv6 addresses.

Parameter	Description
ipv4	Display DNS response-rate-limiting IPv4 entries.
ipv6	Display DNS response-rate-limiting IPv6 entries.

Mode All

Example The following command output shows 15 entries subject to DNS response rate limiting and the number of times each address was contacted:

```
ACOS#show dns response-rate-limiting entries
Source Address          FQDN                        Hit Count
----------------------+---------------------------+----------
10.211.3.101            test4.example.com           4
10.211.3.100            test4.example.com           3
10.211.3.101            test0.example.com           4
10.211.3.100            test0.example.com           4
10.211.3.101            test1.example.com           3
10.211.3.100            test1.example.com           3
10.211.3.101            test3.example.com           3
10.211.3.100            test3.example.com           4
10.211.3.2              test2.example.com           4
10.211.3.2              test4.example.com           4
10.211.3.2              test0.example.com           3
10.211.3.2              test1.example.com           3
10.211.3.2              test3.example.com           4
10.211.3.101            test2.example.com           4
10.211.3.100            test2.example.com           3
Total Entries: 15
```

The following table describes the fields in the command output.

Field	Description
Source Address	IP address initiating the DNS query.
FQDN	Fully qualified domain name that is being resolved.
Hit Count	Total number of DNS queries from the same source address requesting the same FQDN resolution.

Field	Description
Total Entries	Total number of DNS responses subject to rate limiting.

show dns statistics

Description Show DNS statistics.

Syntax

```
show dns {cache {client | entry | statistics} | statistics}
```

Parameter	Description
cache client	Show DNS client statistics.
cache entry	Show DNC cache entry.
cache statistics	Show DNS cache statistics
statistics	Show DNS packet statistics.

Mode Privileged EXEC level and configuration levels

Usage This command lists the DNS traffic statistics.

Example The following command displays DNS statistics:

```
ACOS#show dns statistics
DNS statistics for SLB:
-----------------------
No. of requests: 510
No. of responses: 508
No. of requests with no response: 2
No. of request retransmits: 0
No. of requests and responses not match: 0
No. of resource failures: 0
DNS requests drop: 0
Filter type drop: 0
Filter class drop: 0
Filter type ANY drop: 0
RPZ action drop: 0
RPZ action pass through: 0
RPZ action force switching tcp: 0
```

```
RPZ action nxdomain return: 0
RPZ action nodata return: 0
RPZ action walled garden: 0
DNS statistics for IP NAT:
--------------------------
DNS requests drop: 0
No. of requests: 0
No. of responses: 0
No. of requests with no response: 0
No. of request retransmits: 0
No. of resource failures: 0
No. of requests reusing a transaction id: 0
DNS statistics others:
--------------------------
No. of successful client tls: 0
No. of successful server tls: 0
No. of backend udp conns created: 0
No. of backend udp conns established: 0
No. of paddings to server stripped: 0
No. of paddings to client added: 0
No. of edns client subnet to server removed: 0
No. of udp retransmission: 0
No. of udp retransmission failed: 0
No. of invalid query length to convert to udp from tcp: 0
No. of ECS received from client: 0
No. of ECS inserted: 0
```

The following table describes the fields in the command output.

Field	Description
No. of requests	Number of DNS request received.
No. of responses	Number of DNS response received.
No. of requests with no response	Number of DNS connection that did not received any response.
No. of request retrans-mits	Number of DNS connection receives retransmitted request from client.
No. of requests and responses not match	Number of DNS connection that receives

Field	Description
	different number of requests and responses.
No. of resource failures	Number of times DNS connection gets source NAT resource failed.
DNS requests drop	Dropped DNS requests.
Filter type drop	Number of DNS type query dropped.
Filter class drop	Number of DNS class query dropped.
Filter type ANY drop	Number of DNS ANY-type query dropped by query-type-filter under SLB template DNS.
RPZ action drop	Number of DNS queries dropped due to Response Policy Zone (RPZ) rules.
RPZ action pass through	Number of queries allowed through without action due to RPZ rules.
RPZ action force switching tcp	Number of queries forced to use TCP due to RPZ.
RPZ action nxdomain return	RPZ rule caused DNS server to return NXDOMAIN.
RPZ action nodata return	RPZ rule caused DNS server to return NODATA.
RPZ action walled garden	RPZ redirected DNS query to a walled garden.
DNS requests drop	Dropped requests during IP NAT handling.
No. of requests	Number of DNS request received via NAT.
No. of responses	Number of DNS response received via NAT.
No. of requests with no response	Number of DNS connection that did not receives any response via NAT.

Field	Description
No. of request retrans-mits	Number of DNS connection receives retransmitted request from client via NAT.
No. of resource failures	Number of DNS connection that receives different number of requests and responses via NAT.
No. of requests reusing a transaction id	Number of DNS connection that requests using a previously used DNS transaction ID.
No. of successful client tls	Number of successful DNS-over-TLS ses-sions with clients.
No. of successful server tls	Number of successful DNS-over-TLS ses-sions with servers.
No. of backend udp conns created	Number of UDP connections created to backend servers.
No. of backend udp conns established	Number of successful backend UDP con-nections.
No. of paddings to server stripped	Number of paddings from client query before sending to server.
No. of paddings to client added	Number of paddings added to response for client.
No. of edns client subnet to server removed	Number of EDNS Client Subnet (ECS) info removed before sending to server.
No. of udp retrans-mission	Number of backend UDP retransmission in case of timeout.
No. of udp retrans-mission failed	Number of failed backend UDP retrans-mission.
No. of invalid query length to convert to udp from tcp	Number of failed conversions from TCP to UDP due to query size.
No. of ECS received from	Number of ECS data received from client.

Field	Description
client	
No. of ECS inserted	Number of ECS data added to query before forwarding to server.

show dnssec

Description Show DNS Security Extensions (DNSSEC) information.

show dnssec dnskey

Description Show the DNS Public Key (DNSKEY) resource records for child zones.

Syntax

```
show dnssec dnskey [zone-name]
[all-partitions | partition partition-name]
```

Parameter	Description
zone-name	The name of the child zone. If you do not specify a zone name, DNSKEY resource records for all child zones are displayed.
partition *partition-name*	Display the information for a specific partition.

Mode Privileged EXEC and all configuration levels

show dnssec ds

Description Show the Delegation Signer (DS) resource records for child zones.

Syntax

```
show dnssec ds [zone-name]
[all-partitions | partition partition-name]
```

Parameter	Description
zone-name	The name of the child zone. If you do not specify a

Parameter	Description
	zone name, DS resource records for all child zones are displayed.
partition *partition-name*	Display the information for a specific partition.

Mode Privileged EXEC and all configuration levels

show dnssec statistics

Description Show memory statistics for DNSSEC.

Syntax

```
show dnssec statistics memory
```

Mode Privileged EXEC and all configuration levels

show dnssec status

Description Show the DNSSEC status for each zone.

Syntax

```
show dnssec status
```

Mode Privileged EXEC and all configuration levels

show dnssec template

Description Show DNSSEC templates.

Syntax

```
show dnssec template [default | template-name]
[all-partitions | partition partition-name]
```

Parameter	Description
default | *template-name*	The name of the template. If you do not specify a template name, all DNSSEC templates are displayed.

Parameter	Description
partition partition-name	Display the information for a specific partition.

Mode Privileged EXEC and all configuration levels

show dumpthread

Description Show status information about the system threads.

Syntax

```
show dumpthread
```

Mode Privileged EXEC level and configuration levels

Example Example output for this command:

```
ACOS#show dumpthread
It has been rebooted 1 time.
It has been crashed 0 time.
The process is up 101102 sec.
```

show environment

Description Display temperature, fan, and power supply status.

Syntax

```
show environment
```

Mode All

Example The following command shows environment information for an A10 Thunder Series 3030S device:

NOTE:

- The output on your device may vary from the one shown below.
- ACOS does not trigger a power-off event until the condition is detected three consecutive times. The event is triggered on the fourth detection, and all values follow this trigger event. FAN reports a status (OK or FAIL) and a speed range (low, med, or high). For example: Fan1A : OK-med/high. Low and high speed ranges follow the trigger event, while OK and FAIL statuses are reported immediately.

```
ACOS#show environment
Updated information every 30 Seconds
Physical System temperature:   40C / 104F : OK-low/med
Fan1A : OK-med/high     Fan1B : OK-low/med
Fan2A : OK-med/high     Fan2B : OK-low/med
Fan3A : OK-med/high     Fan3B : OK-low/med
Fan4A : OK-med/high     Fan4B : OK-low/med
System Voltage 12V          : OK
System Voltage 5V           : OK
System Voltage AVCC 3.3V    : OK
System Voltage CC(3.3V)     : OK
System Voltage VCore(0.9v)   : OK
System Voltage VBAT 3.3V    : OK
System Voltage PCH 1.05V    : OK
System Voltage CPU0 VCore   : OK
System Voltage VTT 1.05V    : OK
System Voltage DDR 1.5V     : OK
Right Power Unit(view from front) State: Off
Left Power Unit(view from front) State: On
Power Supply temperature: 36C / 96F
```

show errors

Description Show error information for the system. This command provides a way to quickly view system status and error statistics.

Syntax

```
show errors
[
application [sub-options] |
```

```
critical [detail] |
detail |
informational [detail] |
system [sub-options]
]
```

The exact syntax and sub-options available per command vary; use the ? command at the CLI prompt for available options.

Parameter	Description
application	Display error information for ACOS applications: • **ha** • **hw-compression** • **ipnat** • **l2-l3-forward** • **ram-cache** • **slb** • **ssl**
system	Display error information for ACOS system components: • **hardware** • **software**
informational	Display informational-level errors only.
critical	Display critical-level errors only.
detail	Display detailed error information.

Mode All

Example The following shows high-level error information for the system:

```
ACOS# show errors

Hardware components status
==========================
Physical System temperature: 36C / 96F
CPU Fan1 speed: 5818 RPM
```

```
CPU Fan2 speed: 5720 RPM
Upper Power Unit State: On
Lower Power Unit State: Off

  Total(MB)  Used       Free       Usage
-----------------------------------------
  157065     5777       151287     3.6%

  Device   Primary Disk
------------------------------
  md0      Active
  md1      Active

System Memory Usage:
Total(KB)  Free       Shared     Buffers    Cached     Usage
-----------------------------------------------------------------
----------
2074308    316048     0          37324      256232     72.4%

Time: 21:22:12 IST Mon May 17 2010
            1Sec    5Sec    10Sec   30Sec   60Sec
-------------------------------------------------------
Control      31%     30%     25%     25%     26%
Data1         0%      0%      0%      0%      0%
Data2         0%      0%      0%      0%      0%
Data3         0%      0%      0%      0%      0%
Data4         0%      0%      0%      0%      0%
Data5         0%      0%      0%      0%      0%

System software Error Counters
==========================================
Error packets drops:          : 16
Hardware compression device is not installed.

L2-L3 Fwd (Switch) Error Counters
==========================================
Link Down Drop                : 57
VLAN Flood                    : 175313

Health Monitor Error Counters
```

```
=========================================
Send packet failed:           : 1741315
Retries:                      : 28982
Timeouts:                     : 9
```

Example The following command shows detailed system-software error statistics:

```
ACOS# show errors system software detail

System software Error Counters
=========================================
buff alloc failed:            : 0
buff alloc from sys failed:   : 0
fpga pci read timeout:        : 0
Error packets drops:          : 0
Packet drops:                 : 0
Packets received error:       : 0
```

Example The following command shows detailed error statistics for SLB health monitoring:

```
ACOS# show errors application slb health-monitor detail

Health Monitor Error Counters
=========================================
Open socket failed:           : 0
Send packet failed:           : 1742518
Receive packet failed:        : 0
Unexpected error:             : 0
Retries:                      : 29002
Timeouts:                     : 9
```

The Error packets drops counter indicates the number of packets that were dropped before ACOS applied any load balancing logic, because the contents of the packet were invalid. Some examples:

- Attack packets
- Packets whose IP total length does not correspond with the size of the Ethernet frame

The Packets received error counter is the same as the Error packets drops counter, but does not count packets from the ACOS Linux IP Stack.

The Packet drops counter indicates the number of packets that were dropped because due to a load balancing logic error. As an example, this counter includes packets dropped because the session has been deleted.

show event-action

Description View the events generated for L3V partition creation or deletion as configured by the event command.

Syntax

```
show event-action partition {partition-create | partition-delete}
```

Parameter	Description
partition-create	View partition creation events.
partition-delete	View partition deletion events.

Mode All

Example This example shows the output of this command:

```
ACOS(config)#show event-action vnp part-create
Event VNP part-create action configuration: logging  off,
email  off
```

Related Commands:

- event

show fail-safe

Description Display fail-safe information.

Syntax

```
show fail-safe {config | information}
```

Parameter	Description
config	Displays the fail-safe configuration entered by you or other admins.
information	Displays fail-safe settings and statistics. The output differs between models that use FTAs in hardware and models that do not.

Mode All

Example The following commands configure some fail-safe settings and verify the changes.

```
ACOS(config)#fail-safe session-mem-recovery-threshold 30
ACOS(config)#fail-safe fpga-buff-recovery-threshold 2
ACOS(config)#fail-safe sw-error-recovery-timeout 3
ACOS(config)#show fail-safe config
fail-safe hw-error-monitor-enable
fail-safe session-memory-recovery-threshold 30
fail-safe fpga-buff-recovery-threshold 2
fail-safe sw-error-recovery-timeout 3
```

Example The following command shows fail-safe settings and statistics on an ACOS Device that uses FTAs in hardware:

```
ACOS(config)#show fail-safe information
Total Session Memory (2M blocks):                    1012
Free Session Memory (2M blocks):                     1010
Session Memory Recovery Threshold (2M blocks):       809
Total Configured FPGA Buffers (# of buffers):        4194304
Free FPGA Buffers in Domain 1 (# of buffers):        507787
Free FPGA Buffers in Domain 2 (# of buffers):        508078
Total Free FPGA Buffers (# of buffers):              1015865
FPGA Buffer Recovery Threshold (# of buffers):       256
Total System Memory (Bytes):                         2020413440
```

The following table describes the fields in the command output.

Field	Description
Total	Total amount of the ACOS Device’s memory that is

Field	Description
Session Memory	allocated for session processing.
Free Session Memory	Amount of the ACOS Device's session memory that is free for new sessions.
Session Memory Recovery Threshold	Minimum percentage of session memory that must be free before fail-safe occurs.
Total Configured FPGA Buffers	Total number of configured FTA buffers the ACOS Device has. These buffers are allocated when the ACOS Device is booted. This number does not change during system operation. The FTA device is logically divided into 2 domains, which each have their own buffers. The next two counters are for these logical FTA domains.
Free FPGA Buffers in Domain 1	Number of FTA buffers in Domain 1 that are currently free for new data.
Free FPGA Buffers in Domain 2	Number of FTA buffers in Domain 2 that are currently free for new data.
Total Free FPGA Buffers	Total number of free FTA buffers in both FTA domains.
FPGA Buffer Recovery Threshold	Minimum number of packet buffers that must be free before fail-safe occurs.
Total System Memory	Total size the ACOS Device's system memory.

Example

The following command shows fail-safe settings and statistics on an ACOS Device that does not use FTAs in hardware. (The FTA buffer is an I/O buffer instead.)

```
ACOS(config)#show fail-safe information
```

```
Total Session Memory (2M blocks):                    1018
Free Session Memory (2M blocks):                     1017
Session Memory Recovery Threshold (2M blocks):       305
Total Configured FPGA Buffers (# of buffers):        2097152
Free FPGA Buffers (# of buffers):                    2008322
FPGA Buffer Recovery Threshold (# of buffers):       1280
Total System Memory (Bytes):                         4205674496
```

The following table describes the fields in the command output.

Field	Description
Total Session Memory	Total amount of the ACOS Device's memory that is allocated for session processing.
Free Session Memory	Amount of the ACOS Device's session memory that is free for new sessions.
Session Memory Recovery Threshold	Minimum percentage of session memory that must be free before fail-safe occurs.
Total Configured FPGA Buffers	Total number of configured FTA buffers the ACOS Device has. These buffers are allocated when the ACOS Device is booted. This number does not change during system operation.
Free FPGA Buffers	Number of FTA that are free for new data.
FPGA Buffer Recovery Threshold	Minimum number of packet buffers that must be free before fail-safe occurs.
Total System Memory	Total size the ACOS Device's system memory.

show file-system

Description Display log file information for the specified system directory.

Syntax

```
show file-system [ a10log | syslog | varlog ]
```

Parameter	Description
a10log	Display information for logs present in the **a10log** directory. This directory contains showtech and support files.
syslog	Display information for logs present in the **syslog** directory. This directory contains Linux system logs.
varlog	Display information for logs present in the **varlog** directory. This directory contains ACOS system logs.
|	Output modifiers

Mode All

NOTE: This show command is not supported in L3V partitions.

Example The following command shows the log information for **a10log** system directory:

```
ACOS(config)# show file-system a10log
[a10log] :
total 581M
 60M | showtech08
 56M | .log_mmap2
 18M | showtech14.gz
 18M | showtech13.gz
 18M | showtech12.gz
 18M | showtech11.gz
 17M | showtech10.gz
 17M | showtech09.gz
 17M | showtech08.gz
 17M | showtech18.gz
 16M | showtech19.gz
 16M | showtech31.gz
 16M | showtech30.gz
 16M | showtech15.gz
 16M | showtech16.gz
```

```
15M | showtech28.gz
15M | showtech06.gz
15M | showtech04.gz
15M | showtech05.gz
15M | showtech03.gz
15M | showtech02.gz
15M | showtech01.gz
15M | showtech07.gz
15M | showtech27.gz
14M | showtech26.gz
14M | showtech25.gz
14M | showtech24.gz
14M | showtech23.gz
14M | showtech22.gz
12M | showtech21.gz
11M | showtech20.gz
7.5M | .rpt_summary.dump
7.2M | showtech17.gz
6.8M | showtech29.gz
5.7M | .log_mmap2.ipfix
5.7M | .log_mmap2.priv
294K | a10dpdk.log
220K | a10core.1669821816.7367.6.0.0-d.363
220K | a10core.1669022585.11468.6.0.0-d.363
220K | a10core.1668672797.7000.6.0.0-d.363
73K | url_sftp.log
8.0K | .a10_kernelcore
6.6K | btdump.a10lb.7268
4.0K | rcache
4.0K | slog
4.0K | var
1.9K | up.log
1.2K | initrd.log
689 | url_ftp.log
652 | sync_db.log
380 | httpd_restart_try_python_post.log
303 | guimclog_db.log
252 | update_end_port_zone_service.log
243 | reset_auto_incident.log
242 | delete_level_track.log
```

```
 112 | a10boot.log
 8 | clear.log
 5 | mgmt_if_name
 0 | .rpt_sflow.raw
 0 | authd.log
 0 | del_rrd.log
 0 | reset_cpld_reason
 0 | rrd_clean.log
 0 | url_axfr.log
 0 | url_http.log
 0 | url_https.log
 0 | url_scp.log
 0 | url_tftp.log
[a10log] rcache:
total 0
[a10log] slog:
total 8.0K
 4.0K | scaleout
 4.0K | vcs
[a10log] slog/scaleout:
total 317M
 31M | .infra.slog
 31M | .infra.slog_0
 31M | .infra.slog_1
 31M | .infra.slog_2
 31M | .infra.slog_3
 31M | .infra.slog_4
 31M | .infra.slog_5
 31M | .infra.slog_6
 31M | .infra.slog_7
 31M | .infra.slog_8
 31M | .infra.slog_9
[a10log] slog/vcs:
total 28M
 31M | .a10cfgmgr.slog
 31M | .a10dcs.slog
 31M | .a10lb.slog
 31M | .generic.slog
[a10log] var:
total 4.0K
```

```
 4.0K | ha_shell
 0 | cfgsync_sync_log
[a10log] var/ha_shell:
total 4.0K
 4.0K | config_load
[a10log] var/ha_shell/config_load:
total 0
```

show glid

Description Show information for global IP limiting rules.

Syntax

```
show glid [num]
```

Parameter	Description
num	View configuration information for the specified GLID only.

Mode All

Example The following command the configuration of each global IP limiting rule:

```
ACOS#show glid
glid 1
   conn-limit 100
   conn-rate-limit 100 per 10
   request-limit 1
   request-rate-limit 10 per 10
   over-limit-action reset log 1
glid 2
   conn-limit 20000
   conn-rate-limit 2000 per 10
   request-limit 200
   request-rate-limit 200 per 1
   over-limit-action reset log 3
glid 30
   conn-limit 10000
   conn-rate-limit 1000 per 1
   over-limit-action forward log
```

Example The following command shows the configuration of global IP limiting rule 1:

```
ACOS#show glid 1
glid 1
   conn-limit 100
   conn-rate-limit 100 per 10
   request-limit 1
   request-rate-limit 10 per 10
   over-limit-action reset log 1
```

show gui-image-list

Description Show list of GUI images loaded.

Syntax

```
show gui-image-list | [begin | include | exclude | section]
```

Default All

Mode Global

Example The show GUI image list output is as follows:

```
ACOS#show gui-image-list
GUI Image Pri
------------------------------------------------------------------
---------
N/A
------------------------------------------------------------------
---------
GUI Image Sec
------------------------------------------------------------------
---------
N/A
```

show hardware

Description Displays hardware information for the ACOS Device.

Syntax

```
show hardware [detail | [begin | include | exclude | section]]
LINE
```

Mode All

Default Aggregated summary is displayed by default.

Mode Configuration mode

Usage Use “detail” option for per-port information.

Example Below is a sample output for this command, the output you see may differ depending on your specific platform.

```
ACOS#show hardware
Thunder Series Unified Application Service Gateway TH7650
      Serial No  : TH76500000000002
      CPU        : Intel(R) Xeon(R) Gold 6138T CPU @ 2.00GHz
                   80 cores
                   4 stepping
      Storage    : Total 476G drive
      Memory     : Total System Memory 193602 Mbytes
      SSL Cards  : 6 device(s) present
                   6 QAT SSL device(s)

      L2/3 ASIC  : 3 device(s) present
      IPMI       : IPMI Present
      Ports      : 16
      Flags      : CF
      SMBIOS     : Build  5.14
                    06/11/2019
      FPGA       : 8 instance(s) present
        Date: 07/23/2019
```

show health

Description Show status information for health monitors.

Syntax

```
show health
{
database |
external [name] |
gateway |
monitor [name] |
postfile [name] |
source-nat|
```

```
stat|
[all-partitions | partition {shared | name}]
}
```

Parameter	Description
database	Show the database health check log.
external [*name*]	Shows configuration settings for the specified external health monitoring program.
gateway	Shows configuration settings and statistics for gateway health monitoring.
monitor [*name*]	Shows configuration settings and status for the specified health monitor.
postfile [*name*]	Shows the files used for POST requests in HTTP/HTTPS health checks.
source-nat	Shows health monitor source NAT information.
stat	Shows health monitoring statistics. The statistics apply to all health monitoring activity on the ACOS.

Mode All

Usage To display health monitor information for a specific partition only, use the **partition** *name* option.

Example This command shows configuration settings and status for health monitor “HTTP-7”:

```
ACOS# show health monitor HTTP-7
Monitor Name:           HTTP-7
Interval:               5
Max Retry:              3
Timeout:                5
Up-Retry:               1
Status:                 Idle
Method:                 ICMP
```

```
Attribute:              port=80
                        url="GET /"

Service information:

Service         IP address      Port  Status
Reason(Up/Down)
-------------------------------------------------
-----------------
s4              10.0.0.1         80    UP      HTTP
Status Code OK
ACOS#
```

The output shows the method used for the monitor, and the settings for each of the parameters that are configurable for that method.

Example This command shows configuration settings and status for health monitor “HM”:

```
ACOS(config-slb svc-group)#show health monitor HM
Monitor Name:           HM
Interval:               5
Max Retry:              3
Up-Retry:               1
SSL-Ciphers: DEFAULT
Proxy-Header: v1
Passive Enable
Status:                 In use
Method:                 HTTP
Attribute:              port=80
                        url="GET /"

Service information:

Service         IP address      Port  Status
Reason(Up/Down)
-------------------------------------------------
-----------------------
```

```
s33              10.10.110.33     80     UP       HTTP
Status Code OK
ACOS(config-slb svc-group)#
```

The output shows the proxy header used for the monitor. Proxy header can be used only for TCP, HTTP and HTTPS method types.

Example This command shows configuration settings and status for health monitor “HTTPS”:

```
ACOS#show health https
Total HTTPS number:                        : 2
Total SSL Tickets:                         : 2
Status UP:                                 : 2
Status DOWN:                               : 0
Status UNKN:                               : 0
Status OTHER:                              : 0

IP address      Port  Health monitor Status Version
Ticket Cipher
-------------------------------------------------
------------------
10.212.3.100    443   test-ssl       UP    TLSv1.3
X      TLS_AES_256_GCM_SHA384
10.212.3.100    443   test-ssl2      UP    TLSv1.3
-      TLS_AES_256_GCM_SHA384
```

Example The following command shows the configuration settings of external health monitoring program “http.tcl”:

```
ACOS config#show health external http.tcl
External Program                Description
http.tcl                        check http method
!!! Content Begin !!!
set ax_env(Result) 1

# Open a socket
if {[catch {socket $ax_env(ServerHost) $ax_env
(ServerPort)} sock]} {
   puts stderr "$ax_env(ServerHost): $sock"
```

```
} else {
   fconfigure $sock -buffering none -eofchar {}

   # Send the request
   puts $sock "GET / HTTP/1.0\n"

   # Wait for the response from http server
   set line [read $sock]

   if { [ regexp "HTTP/1.. (\[0-9\]+) " $line
match status] } {
      puts "server $ax_env(ServerHost) response :
$status"
   }
close $sock

   # Check exit code
   if { $status == 200 } {
      set ax_env(Result) 0
   }
}
!!! Content End !!!
```

Example The following command shows the external health monitoring log to get date and time:

```
ACOS config#show health external-log
Sat Feb 15 21:28:21 CET 2025 ### Executing telnet
to 23.23.23.5:0 ###
```

Example The following command shows health monitoring statistics:

```
ACOS#show health stat
Health monitor statistics
Total run time:                          : 2 hours
1345 seconds
Number of burst:                         : 0
max scan jiffie:                         : 326
min scan jiffie:                         : 1
average scan jiffie:                     : 1
```

```
Opened socket:                              : 1140
Open socket failed:                         : 0
Close socket:                               : 1136
Send packet:                                : 0
Send packet failed:                         : 259379
Receive packet:                             : 0
Receive packet failed                       : 0
Retry times:                                : 4270
Timeout:                                    : 0
Unexpected error:                           : 0
Conn Immediate Success:                     : 0
Socket closed before l7:                    : 0
Socket closed without fd notify:            : 0
Configured health-check rate (/500ms)   : Auto
configured
Current health-check rate (/500ms):     : 1600
External health-check max rate(/200ms) : 2
Total number:                               : 8009
Status UP:                                  : 8009
Status DOWN:                                : 0
Status UNKN:                                : 0
Status OTHER:                               : 0

IP address      Port  Health monitor  Status Cause
(Up/Down) Reason (UP/DOWN)               Retry PIN
-------------------------------------------------
---------------------------------------
10.0.0.11       80    http             UP     11 /0  @0       0
 0 0/0 0
10.0.0.12       80    http             UP     10 /0  @0       0
 0 0/0 0
10.168.10.19 3306  mysql               UP     2  /23 @1
External Script Report Up 0 0/0 0
14.14.14.22 1521  oracle               UP     2  /0  @0
External Script Report Up 1 0/0 0
3030::14         3306 default           UP     2  /0  @0
ICMPv6           0 0/0 0
```

The following table describes the fields in the command output.

Field	Description
Total run time	Time elapsed since the health monitoring process started.
Number of burst	Number of times the system detected that a health check would leave the ACOS device as a traffic burst, and remedied the situation.
max scan jiffie	These are internal counters used by technical support for debugging purposes.
min scan jiffie	
average scan jiffie	
Opened socket	Number of sockets opened.
Open socket failed	Number of failed attempts to open a socket.
Close socket	Number of sockets closed.
Send packet	Number of health check packets sent to the target of the health monitor.
Send packet failed	Number of sent health check packets that failed. (This is the number of times a target server or service failed its health check.)
Receive packet	Number of packets received from the target in reply to health checks.
Receive packet failed	Number of failed receive attempts.
Retry times	Number of times a health check was resent because the target did not reply.

Field	Description
Timeout	Number of times a response was not received before the health check timed out.
Unexpected error	Number of unexpected errors that occurred.
Conn Immediate Success	These are internal counters used by technical support for debugging purposes.
Socket closed before l7	
Socket closed without fd notify	
Configured health-check rate	If auto-adjust is enabled, shows “Auto configured”. If auto-adjust is disabled, shows the manually configured threshold.
Current health-check rate	If auto-adjust is enabled, shows the total number of health monitors divided by the global health-check timeout: `total-monitors / global-timeout` If auto-adjust is disabled, shows the manually configured threshold.
External health-check max rate	The external health-check probe rate.
Total number	Total number of health checks performed.

Field	Description
Status UP	Number of health checks that resulted in status UP.
Status DOWN	Number of health checks that resulted in status DOWN.
Status UNKN	Number of health checks that resulted in status UNKN.
Status OTHER	Number of health checks that resulted in status OTHER.
IP address	IP address of the real server.
Port	Protocol port on the server.
Health monitor	Name of the health monitor. If the name is “default”, the default health monitor settings for the protocol port type are being used. (See “health-check” in the *Command Line Interface Reference for ADC* for Layer 3 health checks or “port” in the *Command Line Interface Reference for ADC*for Layer 4-7 health checks.)
Status	Indicates whether the service passed the most recent health check.
Cause (Up/Down)	Up and Down show internal codes for the reasons the health check reported the server or service to be up or down.
Reason (Up/Down)	Reason that caused the Up / Down status.
Retry	Number of retries.
PIN	Indicates the following: • Current number of retries – Displayed to the left of the slash (/).

Field	Description
	The number of times the most recent health check was retried before a response was received or the maximum number of retries was used. • Current successful up-retries – Displayed to the right of the slash (/). Number of successful health check replies received for the current health check. This field is applicable if the **up-retry** option is configured for the health check. (See health monitor.)

Example The following command shows health monitoring source NAT statistics:

```
ACOS#show health source-nat statistics

otal
-------------------------------------------------
-----
Packets received from standby                  0
Packets sent to standby                        0
Packets received from active                   0
Packets sent to active                         0
Packets received from active error             0
Packets received from kernel                   0
Packets sent to kernel                         0
Packets sent to kernel error                   0
Peer not found on standby                      0
DCMSG error                                    0
SLB object not found                           0
Smart NAT port initialization error            0
Smart NAT instance initialization error        0
Smart NAT SLB server route update error        0
Smart NAT SLB server ip update error           0
```

```
NAT resource error                                  0
```

The following table describes the fields in the command output.

Field	Description
Packets received from standby	Number of packets received from the standby device in VRRP-A mode.
Packets sent to standby	Number of packets sent to the standby device in VRRP-A mode.
Packets received from active	Number of packets received from the active device in VRRP-A mode.
Packets sent to active	Number of packets sent to the active device in VRRP-A mode.
Packets received from active error	Error occurred while receiving packets from the active device in VRRP-A mode.
Packets received from kernel	Number of packets received from the health check module.
Packets sent to kernel	Number of packets sent to the health check module.
Packets sent to kernel error	Error occurred when sending packets to health check module.
Peer not found on standby	No peer found on standby device to forward health check traffic.
DCMSG error	Direct Control Message (DCMSG) error.
SLB object not found	No corresponding SLB object found for the health check process.
Smart NAT port initialization error	Error initializing Smart NAT port.

Field	Description
Smart NAT instance initialization error	Error initializing the Smart NAT instance.
Smart NAT SLB server route update error	Smart NAT failed to update the route to the SLB server.
Smart NAT SLB server ip update error	Smart NAT failed to update the IP to the SLB server.
NAT resource error	NAT resources cannot allocate for the source NAT operation.

show history

Description Show the CLI command history for the current session.

Syntax

```
show history
```

Mode Privileged EXEC level and configuration levels

Usage Commands are listed starting with the oldest command, which appears at the top of the list.

Example The following example shows a history of CLI commands (truncated for brevity):

```
ACOS#show history
  enable
  show version
  show access-list
  show admin
  show admin admin
  show admin detail
  show admin session
...
```

show icmp

Description Show ICMP rate limiting configuration settings and statistics.

Syntax

```
show icmp [stats]
```

Use the **stats** option to view detailed statistics.

Mode All

Example The following command shows ICMP rate limiting settings, and the number of ICMP packets dropped because the threshold has been exceeded:

```
ACOS(config)#show icmp
Global rate limit:                          5
Global lockup rate limit:                   10
Lockup period:                              20
Current global rate:                        0
Global rate limit drops:                    0
Interfaces rate limit drops:                0
Virtual server rate limit drops:            0
Total rate limit drops:                     0
```

show icmpv6

Description Show ICMPv6 rate limiting configuration settings and statistics.

Syntax

```
show icmpv6 [stats]
```

Use the **stats** option to view detailed statistics.

Mode All

show interfaces

Description Displays interface configuration and status information.

Syntax

```
show interfaces
[brief] |
[ethernet [num]] |
[ve [num]] |
```

```
[lif num] |
[loopback num] |
[management] |
[management2] |
[trunk [num] |
[tunnel [num]] |
[media] |
[statistics] |
[transceiver]
```

Mode Privileged EXEC level and configuration levels

Usage If no specific interface type and number are specified, statistics for all configured interfaces are displayed.

Example The following example shows information for Ethernet port 9:

```
ACOS#show interfaces ethernet 9
Ethernet 9 is up, line protocol is up
Hardware is 10Gig, Address is 001f.a008.0fba
Unnumbered is configured and active, peer is
fe80::21f:a0ff:fe07:635a
Internet address is 0.0.0.0, Subnet mask is 0.0.0.0
IPv6 link-local address is fe80::21f:a0ff:fe08:fba Prefix 64
Type: Link-Local
Configured Speed auto, Actual 10Gbit, Configured Duplex auto,
Actual fdx
Member of L2 Vlan 1, Port is Untagged
Flow Control is disabled, IP MTU is 1500 bytes
Port as Mirror disabled, Monitoring this Port disabled
Interface name is IBGP-to-SLBAX1-L3v
7675141 packets input 950488101 bytes
Received 0 broadcasts, Received 9867 multicasts, Received
7665274
unicasts
0 input errors 0 CRC 0 frame
0 runts 0 input giants
9968713 packets output 922172489 bytes
Transmitted 0 broadcasts, Transmitted 9895 multicasts,
Transmitted
9958818 unicasts
0 output errors 0 output giants 0 collisions
300 second input rate: 11424 bits/sec, 11 packets/sec, 0%
utilization
```

```
300 second output rate: 16440 bits/sec, 20 packets/sec, 0%
utilization
```

Example The following example shows information for loopback interface 8:

```
ACOS#show interfaces loopback 8
Loopback 8 is up, line protocol is up
  Hardware is Loopback
  Internet address is 10.10.10.55, Subnet mask is
255.255.255.0
```

Example The following example shows Virtual Ethernet (VE) interface statistics:

```
ACOS#show interfaces ve 10
VirtualEthernet 10 is up, line protocol is up
  Hardware is VirtualEthernet, Address is 001f.a004.c0e2
  Internet address is 110.10.10.1, Subnet mask is
255.255.255.0
  IPv6 address is 2001:10::241 Prefix 64 Type: unicast
  IPv6 link-local address is fe80::21f:a0ff:fe04:c0e2 Prefix
64 Type: unicast
  Router Interface for L2 Vlan 10
  IP MTU is 1500 bytes
  28 packets input  2024 bytes
  Received  0 broadcasts, Received 24 multicasts, Received 4
unicasts
  10 packets output  692 bytes
  Transmitted  8 broadcasts, Transmitted 2 multicasts,
Transmitted 0 unicasts
  300 second input rate: 48 bits/sec, 0 packets/sec
  300 second output rate: 16 bits/sec, 0 packets/sec
```

Example The following example shows information for logical interface 124:

```
ACOS(config-if:lif:124)#show int lif 124
lif 124 is up, line protocol is up
Logical interface Lif, Address is 625d.d6f7.206b
IP Unnumbered is configured and active
IP Encap, Local endpoint 165.165.165.2, Remote endpoint
165.165.165.1
IP MTU is 1500 bytes
0 packets input  0 bytes
```

```
Received  0 broadcasts, Received 0 multicasts, Received 0
unicasts
0 packets output  0 bytes
Transmitted  0 broadcasts, Transmitted 0 multicasts,
Transmitted 0 unicasts
```

Example The following example shows information for the interface management:

```
ACOS#show interface management
Management 0 is up, line protocol is up.
Hardware is 10Gig, Address is 001f.a044.7167
Internet address is 10.65.21.80, Subnet mask is 255.255.255.0
Configured Speed 1000, Actual 1000, Configured Duplex fdx,
Actual fdx
Flow Control is disabled, IP MTU is 1500 bytes
22072 packets input,  2283580 bytes
Received 21642 broadcasts,  Received 181 multicasts,  Received
249 unicasts
0 input errors,  0 CRC  0 frame
0 runts  0 giants
369 packets output  45195 bytes
Transmitted 17 broadcasts  29 multicasts  323 unicasts
0 output errors  0 collisions
```

Example The following example shows information for the second interface management (management2). The information for the second management is displayed only for the Thunder 8665S platform:

```
ACOS#show interface management2
Management 2 is up, line protocol is up
Hardware is 10Gig, Address is 001f.a044.7166
Internet address is 10.65.28.62, Subnet mask is 255.255.255.0
Internet V6 address is 1111::1/64
IPv6 link-local address is fe80::200:ff:fe00:0/64
Configured Speed N/A, Actual 1000, Configured Duplex N/A,
Actual Full
Flow Control is disabled,IP MTU is 1500 bytes
23922 packets input,  2448254 bytes
Received 21648 broadcasts,  Received 602 multicasts,  Received
1672 unicasts
```

```
0 input errors,  0 CRC  0 frame
0 runts  0 giants
1690 packets output  214668 bytes
Transmitted 12 broadcasts  24 multicasts  1654 unicasts
0 output errors  0 collisions
```

Example The following example shows L2 trunk interface statistics:

```
ACOS#show interfaces trunk 1
Trunk 1 is down, line protocol is down
 Members: 4
 0 packets input  0 bytes
 Received  0 broadcasts, Received 0 multicasts, Received 0
unicasts
 0 packets output  0 bytes
 Transmitted  0 broadcasts, Transmitted 0 multicasts,
Transmitted 0 unicasts
```

Example The following example shows L3 trunk interface statistics:

```
ACOS(config-if:trunk:1)#show interfaces trunk 2
Trunk 1 is down, line protocol is down
 Hardware is TrunkGroup, Address is 001f.a020.04db
 Internet address is 34.34.34.34, Subnet mask is 255.255.255.0
 IP MTU is 1500 bytes
 0 packets input  0 bytes
 Received  0 broadcasts, Received 0 multicasts, Received 0
unicasts
 0 packets output  0 bytes
 Transmitted  0 broadcasts, Transmitted 0 multicasts,
Transmitted 0 unicasts
```

Example The following example shows tunnel interface statistics:

```
ACOS#show interfaces tunnel
Tunnel 1 is up, line protocol is up
  Tunnel interface, Address is 000c.2999.3b37
  Internet address is 1.1.1.2, Subnet mask is 255.255.255.0
  IP MTU is 1500 bytes
  Received      72340 packets   6944640 bytes
    Errors      0
  Transmitted   55353 packets   5313888 bytes
    Errors      0
  300 second input rate: 77432 bits/sec, 100 packets/sec
  300 second output rate: 59048 bits/sec, 100 packets/sec
```

- show interfaces brief
- show interfaces media
- show interfaces statistics
- show interfaces transceiver

show interfaces brief

Description View brief interface information.

Syntax

```
show interfaces brief [ipv6]
```

Mode Privileged EXEC level and configuration levels

Example The following is the example output of the **show interfaces brief** command. The “Flags” column indicates “U” if the BGP protocol is configured with an unnumbered interface and the interface is operational.

```
Port Link  Dupl  Speed Trunk Vlan MAC             IP Address
    IPs Flag Name
-------------------------------------------------------------
--------------------
mgmt Up    Full  1000  N/A   N/A  001f.a008.0fb0
10.65.19.117/24 1
1    Up    Full  10000 none  1     001f.a008.0fb2 8.8.8.8/24      1
2    Disb None  None  none  1     001f.a008.0fb3 0.0.0.0/0       0
3    Disb None  None  none  1     001f.a008.0fb  0.0.0.0/0       0
4    Disb None  None  none  1     001f.a008.0fb5 0.0.0.0/0       0
```

```
5     Disb None   None   none   1      01f.a008.0fb6   0.0.0.0/0          0
6     Disb None   None   none   1      001f.a008.0fb7  0.0.0.0/0          0
7     Disb None   None   none   1      001f.a008.0fb8  0.0.0.0/0          0
8     Disb None   None   none   1      001f.a008.0fb9  0.0.0.0/0          0
9     Up   Full   10000  none   1      001f.a008.0fba  0.0.0.0/0          0
 U
10    Disb None   None   none   1      001f.a008.0fbb  0.0.0.0/0          0
11    Disb None   None   none   1      001f.a008.0fbc  0.0.0.0/0          0
12    Disb None   None   none   1      001f.a008.0fbd  0.0.0.0/0          0
13    Up   Full   10000  6      1      001f.a008.0fbe  0.0.0.0/0          0
14    Up   Full   10000  6      1      001f.a008.0fbf  0.0.0.0/0          0
15    Disb None   None   none   1      001f.a008.0fc0  0.0.0.0/0          0
16    Down None   None   none   1      001f.a008.0fc1  0.0.0.0/0          0
17    Disb None   None   none   1      001f.a008.0fc2  0.0.0.0/0          0
18    Disb None   None   none   1      001f.a008.0fc3  0.0.0.0/0          0
19    Disb None   None   none   1      001f.a008.0fc4  0.0.0.0/0          0
20    Disb None   None   none   1      001f.a008.0fc5  0.0.0.0/0          0
lo1   Up   N/A    N/A    N/A    N/A    N/A             4.4.4.4/32        1
lo2   Up   N/A    N/A    N/A    N/A    N/A             5.5.5.1/24        1
```

Example

The following is the example output of the **`show interfaces brief`** command. The “Flags” column indicates “U” if the Logical Interface (LIF) is configured as an unnumbered interface.

```
Port     Link   Dupl   Speed   Trunk Vlan Encap MAC               IP
Address        IPs Flags   Name
-------------------------------------------------------------------
--------------------------------
mgmt     Up     auto   auto    N/A   N/A  N/A   728a.41ab.c4b7
10.64.19.105/24   1
1        Up     Full   10000   none  Tag  N/A   7283.3fa5.cf02
0.0.0.0/0         0
2        Up     Full   10000   none  Tag  N/A   625d.d6f7.206b
0.0.0.0/0         0
3        Disb   None   None    none  1    N/A   5a1f.6334.0f6e
57.1.1.20/24      1
4        Up     Full   10000   none  1    N/A   8a52.7e33.a4ea
56.1.1.13/24      1
lif 124  Up     N/A    N/A     N/A   1    N/A   625d.d6f7.206b
0.0.0.0/0         0    U
```

```
lif_1    Up     N/A   N/A     N/A   1     N/A   5a1f.6334.0f6e
0.0.0.0/0         0    U
ve2      Up     N/A   N/A     N/A   2     N/A   7283.3fa5.cf02
2.2.2.1/24        1
ve102    Up     N/A   N/A     N/A   102   N/A   625d.d6f7.206b
102.102.102.1/24 1
Global Throughput:0 bits/sec (0 bytes/sec)
Throughput:0 bits/sec (0 bytes/sec)
```

Example The following is the example output of the **show interfaces brief** command. The second management (mgmt2) details are displayed only for the Thunder 8665S platform:

```
Port     Link   Dupl   Speed   Trunk Vlan Encap MAC              IP
Address       IPs Flags   Name
-----------------------------------------------------------------
-----------------------------------------------
mgmt     Up     Full   1000    N/A   N/A  N/A   001f.a044.7167
10.65.21.80/24   1
mgmt2    Up     Full   1000    N/A   N/A  N/A   001f.a044.7166
10.65.28.62/24   1
1        Disb   None   None    none  1    N/A   001f.a044.716f
0.0.0.0/0         0
2        Disb   None   None    none  1    N/A   001f.a044.7170
0.0.0.0/0         0
3        Disb   None   None    none  1    N/A   001f.a044.7171
0.0.0.0/0         0
4        Disb   None   None    none  1    N/A   001f.a044.7172
0.0.0.0/0         0
5        Disb   None   None    none  1    N/A   001f.a044.7173
0.0.0.0/0         0
6        Disb   None   None    none  1    N/A   001f.a044.7174
0.0.0.0/0         0
7        Disb   None   None    none  1    N/A   001f.a044.7175
0.0.0.0/0         0
8        Disb   None   None    none  1    N/A   001f.a044.7176
0.0.0.0/0         0
9        Disb   None   None    none  1    N/A   001f.a044.7177
0.0.0.0/0         0
```

```
10      Disb  None  None   none  1    N/A   001f.a044.7178
0.0.0.0/0       0
11      Disb  None  None   none  1    N/A   001f.a044.7179
0.0.0.0/0       0
12      Disb  None  None   none  1    N/A   001f.a044.717a
0.0.0.0/0       0

Global Throughput:0 bits/sec (0 bytes/sec)
Throughput:0 bits/sec (0 bytes/sec)
```

show interfaces media

Description Display information about 1-Gbps and 10-Gbps small form-factor pluggable (SFP+) interfaces.

Syntax **show interfaces media** [**ethernet** *num*]

Parameter	Description
num	Show information for the specified interface only.

Mode Privileged EXEC level and configuration levels

Usage On VCS, this command provides device-specific media information.

On non-FTA platforms, this command displays the following message,

```
Show interface media feature is not supported on this port
```

This indicates that either no SFP device is detected on the port or the port does not support **show interface media** feature.

NOTE: This command does not show information on media installed in ports that belong to an L3V partition. On platforms that do not have a 1 Gigabit Ethernet port installed, on FTA platforms, or on a virtual appliance model, the following message is displayed when you issue the **show interfaces media** command:

```
No SFP/SFP+ ports found in this model.
```

Example The following example sample output for this command. The example displays output on ports with an installed 1 Gigabit SFP and a 10 Gigabit SFP+ module. When an SFP is not installed, or if the port has not been enabled, an error message appears in the output, as shown below:

```
ACOS-Active# show interfaces media
port 10:
Type:   SFP 1000BASE-SX
Vendor: JDS UNIPHASE
Part#:  JSH-21S3AB3      Serial#:F549470401B0

port 11:
No media detected.

port 18:
Type:   SFP+ 10G Base-SR
Vendor: FINISAR CORP.
Part#:  FTLX8571D3BCL    Serial#:UG505PM

port 19:
No media detected.

port 20:
Cannot retrieve media information when port is disabled.
```

In this example, the SFP+ interface for port 18 is installed and its link is up. The other 10-Gbps interfaces either are down or do not have an SFP+ installed.

Example The following example shows the CLI response if you enter **`show interfaces media`** on an ACOS Device that does not support SFP+ interfaces:

```
ACOS# show interfaces media
No 10G fiber port installed.
```

show interfaces statistics

Description Displays interface statistics.

Syntax

```
show interfaces statistics
[ethernet portnum ]
[{in-pps | in-bps | in-util | out-pps | out-bps | out-util}]
```

Parameter	Description
ethernet *portnum*	Ethernet data interface numbers for which to display statistics. If you omit this option, statistics are displayed for all Ethernet data interfaces and logical tunnel interfaces.
in-pps	Inbound traffic, in packets per second (PPS).
in-bps	Inbound traffic, in bytes per second (BPS).
in-util	Inbound traffic utilization.
out-pps	Outbound traffic, in packets per second (PPS).
out-bps	Outbound traffic, in bytes per second (BPS).
out-util	Outbound traffic utilization.

Mode Privileged EXEC level and configuration levels

Example The following example shows information for interfaces statistics:

```
ACOS#show interfaces statistics
Port InPPS  InBPS InUtil OutPPS OutBPS OutUtil Time
-------------------------------------------------------
1    0.00   1.00  0.00   0.00   1.00   0.00    20:53:55
2    0.00   0.00  0.00   0.00   0.00   0.00    20:53:55
3    0.00   0.00  0.00   0.00   0.00   0.00    20:53:55
4    0.00   0.00  0.00   0.00   0.00   0.00    20:53:55
-------------------------------------------------------
Tot  0.00   1.00  0.00   0.00   1.00   0.00    20:53:55
```

show interfaces transceiver

Description View interface transceiver information for FINISAR 40G and 100G ports.

NOTE: This command is supported only on FTA devices.

Syntax

```
show interfaces transceiver [ethernet num] [details]
```

Mode Privileged EXEC level and configuration levels

Example View information for all configured 40G and 100G ports with the **show interfaces transceiver** command:

```
ACOS#show interfaces transceiver
Optical      Optical
        Temperature  Voltage      Current      Tx Power     Rx
Power
Port    (Celsius)    (Volts)      (mA)         (dBm)
(dBm)
------- -----------  -------      --------     --------     --
------
5       34.83        6.16         16.00        31.35
31.35
6       35.24        6.17         15.00        31.78
31.78
7       46.71        6.18         17.00        32.19
32.19
8       35.78        6.13         15.00        31.78
31.78
9       34.29        6.14         15.00        32.58
32.58
13      40.10        6.13         0.00         0.00
0.00
14      39.42        6.16         0.00         0.00
0.00
```

Example View detailed information for a specific 40G or 100G interface:

```
ACOS#show interfaces transceiver ethernet 5 details
                    High Alarm   High Warn    Low Warn
Low Alarm
        Temperature  Threshold    Threshold    Threshold
Threshold
Port    (Celsius)    (Celsius)    (Celsius)    (Celsius)
(Celsius)
------- -----------  ----------   ---------    ---------    --
-------
5       35.24        84.24        78.84        -8.64        -
14.04
```

```
                    High Alarm   High Warn    Low Warn
Low Alarm
        Voltage     Threshold    Threshold    Threshold
Threshold
Port    (Volts)     (Volts)      (Volts)      (Volts)
(Volts)
------- ----------  ----------   ---------    ---------    --
-------
5       6.16        6.91         6.72         5.62
5.42

                    High Alarm   High Warn     Low Warn
Low Alarm
        Current     Threshold    Threshold     Threshold
Threshold
Port    (mA)        (mA)         (mA)          (mA)
(mA)
------- ----------  ----------   ---------     ---------    --
-------
5       16.00       23.00        21.00         9.00
7.00

        Optical     High Alarm   High Warn    Low Warn
Low Alarm
        TX Power    Threshold    Threshold    Threshold
Threshold
Port    (dBm)       (dBm)        (dBm)        (dBm)
(dBm)
------- ---------   ----------   ---------    ---------    --
-------
5       31.35       34.97        32.96        24.85
23.98

        Optical     High Alarm   High Warn     Low Warn
Low Alarm
        RX Power    Threshold    Threshold     Threshold
Threshold
```

```
Port     (dBm)          (dBm)          (dBm)          (dBm)
(dBm)
------- ---------     ----------    ---------      ---------     -
--------
5        31.35         36.64         34.34         0.00
0.00
```

show ip

Description Show the IP mode in which the ACOS Device is running, gateway or transparent mode.

Syntax

```
show ip
```

Mode All

Example The following command shows that the ACOS Device is running in gateway mode:

```
ACOS#show ip
System is running in Gateway Mode
```

show ip anomaly-drop statistics

Description Show drop statistics for malformed IP packets.

Syntax

```
show ip anomaly-drop statistics
```

Mode All

Example The following example shows ip anomaly-drop statistics:

```
ACOS#show ip anomaly-drop statistics
IP Anomaly Drop Statistics
--------------------------
```

```
Land Attack Drop                        0
Empty Fragment Drop                     0
Micro Fragment Drop                     0
IPv4 Options Drop                       0
IP Fragment Drop                        0
Bad IP Header Len Drop                  0
Bad IP Flags Drop                       0
Bad IP TTL Drop                         0
No IP Payload drop                      0
Oversize IP Payload Drop                0
Bad IP Payload Len Drop                 0
Bad IP Fragment Offset Drop             0
Bad IP Checksum Drop                    0
ICMP Ping of Death Drop                 0
TCP Bad Urgent Offset Drop              0
TCP Short Header Drop                   0
TCP Bad IP Length Drop                  0
TCP Null Flags Drop                     0
TCP Null Scan Drop                      0
TCP Syn and Fin Drop                    0
TCP XMAS Flags Drop                     0
TCP XMAS Scan Drop                      0
TCP Syn Fragment Drop                   0
TCP Fragmented Header Drop              0
TCP Bad Checksum Drop                   0
UDP Short Header Drop                   0
UDP Bad Length Drop                     0
UDP Kerberos Fragment Drop              0
UDP Port Loopback Drop                  0
UDP Bad Checksum Drop                   0
Runt IP Header Drop                     0
Runt TCP/UDP Header Drop                0
IP-over-IP Tunnel Mismatch Drop         0
TCP Option Error Drop                   0
IP-over-IP Tunnel Error Drop            0
VXLAN Tunnel Error Drop                 0
GRE Tunnel Error Drop                   0
GRE PPTP Error Drop                     0
```

```
IPv6 Hop by Hop Header Drop          0
IPv6 Destination Header Drop         0
IPv6 Routing Header Drop             0
IPv6 Fragmentation Header Drop       0
IPv6 Authentication Header Drop      0
IPv6 ESP Header Drop                 0
IPv6 Mobility Header Drop            0
IPv6 No Next Header Drop             0
IPv6 Unknown Extension Header Drop   0
IPv6 Malformed Extension Header Drop 0
```

The following table describes the fields in the command output:

Field	Description
Land Attack Drop	Number of packets dropped due to land attack attempts.
Empty Fragment Drop	Number of packets dropped due to empty IP fragments.
Micro Fragment Drop	Number of packets dropped due to very small IP fragments.
IPv4 Options Drop	Number of packets dropped due to the presence of IPv4 options.
IP Fragment Drop	Number of packets dropped due to malformed or unexpected IP fragmentation.
Bad IP Header Len Drop	Number of packets dropped due to an invalid IP header length.
Bad IP Flags Drop	Number of packets dropped due to incorrect or unexpected IP flag settings.
Bad IP TTL Drop	Number of packets dropped due to an invalid or low TTL (Time-To-Live) value.
No IP Payload Drop	Number of packets dropped due to missing or empty IP payload.
Oversize IP Payload Drop	Number of packets dropped due to an IP payload exceeding the allowed size.
Bad IP Payload Len	Number of packets dropped due to an

Field	Description
Drop	incorrect IP payload length.
Bad IP Fragment Offset Drop	Number of packets dropped due to an invalid IP fragment offset.
Bad IP Checksum Drop	Number of packets dropped due to an incorrect IP checksum.
ICMP Ping of Death Drop	Number of packets dropped due to an ICMP Ping of Death attack attempt.
TCP Bad Urgent Offset Drop	Number of packets dropped due to an invalid TCP urgent pointer offset.
TCP Short Header Drop	Number of packets dropped due to a TCP header shorter than the minimum size.
TCP Bad IP Length Drop	Number of packets dropped due to an incorrect IP length in a TCP packet.
TCP Null Flags Drop	Number of packets dropped due to TCP packets with no flags set.
TCP Null Scan Drop	Number of packets dropped due to TCP null scan attack attempts.
TCP Syn and Fin Drop	Number of packets dropped due to TCP packets containing both SYN and FIN flags.
TCP XMAS Flags Drop	Number of packets dropped due to TCP packets with unusual flag combinations (XMAS scan).
TCP XMAS Scan Drop	Number of packets dropped due to TCP XMAS scan attack attempts.
TCP Syn Fragment Drop	Number of packets dropped due to fragmented TCP SYN packets.
TCP Fragmented Header Drop	Number of packets dropped due to fragmented TCP headers.
TCP Bad Checksum Drop	Number of packets dropped due to an incorrect TCP checksum.
UDP Short Header	Number of packets dropped due to UDP

Field	Description
Drop	headers shorter than expected.
UDP Bad Length Drop	Number of packets dropped due to an invalid UDP length field.
UDP Kerberos Fragment Drop	Number of packets dropped due to fragmented Kerberos UDP traffic.
UDP Port Loopback Drop	Number of packets dropped due to UDP packets with loopback port configurations.
UDP Bad Checksum Drop	Number of packets dropped due to an incorrect UDP checksum.
Runt IP Header Drop	Number of packets dropped due to an IP header shorter than expected.
Runt TCP/UDP Header Drop	Number of packets dropped due to TCP or UDP headers shorter than expected.
IP-over-IP Tunnel Mismatch Drop	Number of packets dropped due to mismatched IP-over-IP tunneling parameters.
TCP Option Error Drop	Number of packets dropped due to invalid or unsupported TCP options.
IP-over-IP Tunnel Error Drop	Number of packets dropped due to errors in IP-over-IP tunneling.
VXLAN Tunnel Error Drop	Number of packets dropped due to VXLAN tunnel configuration issues.
GRE Tunnel Error Drop	Number of packets dropped due to errors in GRE tunnel processing.
GRE PPTP Error Drop	Number of packets dropped due to errors in GRE PPTP tunneling.
IPv6 Hop-by-Hop Header Drop	Number of packets dropped due to IPv6 Hop-by-Hop extension headers.
IPv6 Destination Header Drop	Number of packets dropped due to IPv6 destination options headers.
IPv6 Routing Header Drop	Number of packets dropped due to IPv6 routing extension headers.

Field	Description
IPv6 Fragmentation Header Drop	Number of packets dropped due to IPv6 fragmentation headers.
IPv6 Authentication Header Drop	Number of packets dropped due to IPv6 authentication headers.
IPv6 ESP Header Drop	Number of packets dropped due to IPv6 Encapsulating Security Payload (ESP) headers.
IPv6 Mobility Header Drop	Number of packets dropped due to IPv6 mobility headers.
IPv6 No Next Header Drop	Number of packets dropped due to IPv6 packets missing a next header.
IPv6 Unknown Extension Header Drop	Number of packets dropped due to unknown IPv6 extension headers.
IPv6 Malformed Extension Header Drop	Number of packets dropped due to malformed IPv6 extension headers.

show ip bgp

Description Displays BGP information.

Syntax

```
show ip bgp
```

Mode All

Example The following example shows the BGP IPv4 routes that are learned from the IPv6 global peers:

```
ACOS(config)# show ip bgp
BGP Address Family IPv4 Unicast
BGP table version is 238, local router ID is 200.200.200.200
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal,                          l - labeled S Stale,
m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network          Next Hop                            Metric
  LocPrf Weight Type Path
*> 3.3.3.3/32    4f90::4(fe80::20c:29ff:feab:1b09) ethernet 2
     0      0    64512 i
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet 2
     0      0    64512 i
*> 4.4.4.4/32    4f90::4(fe80::20c:29ff:feab:1b09) ethernet
2      0      0    64512 ?
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet
2      0      0    64512 ?
*> 192.3.3.1/32  4f90::4(fe80::20c:29ff:feab:1b09) ethernet
2      0      0    64512 ?
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet
2      0      0    64512 ?
*> 192.3.3.2/32  4f90::4(fe80::20c:29ff:feab:1b09) ethernet
2      0      0    64512 ?
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet 2
     0      0    64512 ?
*> 192.3.3.3/32  4f90::4(fe80::20c:29ff:feab:1b09) ethernet
2      0      0    64512 ?
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet
2      0      0    64512 ?
*> 192.3.3.4/32  4f90::4(fe80::20c:29ff:feab:1b09) ethernet
2      0      0    64512 ?
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet
2      0      0    64512 ?
*> 192.3.3.5/32  4f90::4(fe80::20c:29ff:feab:1b09) ethernet 2
     0      0    64512 ?
*m               4f90::3(fe80::20c:29ff:fe99:3b19) ethernet 2
```

show ip dns

Description Display system DNS information created by "ip dns {primary | secondary}".

Syntax

```
show ip dns
```

Mode All

Example The following example shows example output for this command.

```
ACOS#show ip dns
DNS suffix: ourcorp
Primary server: 10.10.20.25
Secondary server: 192.168.1.25
```

Related Commands:

ip dns

show ip dns-cache

Description Displays DNS caching information created by "ip dns {primary | secondary}".

Syntax

```
show ip dns-cache
```

Mode All

Example The following example shows example output for this command.

```
ACOS#show ip dns-cache
Total: 0
```

Related Commands:

ip dns

show ip fib | show ipv6 fib

Description Display Forwarding Information Base (FIB) entries.

NOTE: This command is applicable only on ACOS Devices that are configured in route mode. The command returns an error if you enter it on a device configured for transparent mode.

Syntax

```
show {ip | ipv6} fib
```

Mode All

Example The following command shows the IPv4 and IPv6 FIB entries on an ACOS Device configured in route mode:

```
ACOS#show ip fib
Prefix                  Next Hop        Interface
Distance
-------------------------------------------------------------------
----------
0.0.0.0 /0              192.168.20.1    ve10            0
192.168.20.0 /24        0.0.0.0         ve10            0
Total routes = 2
```

Example The following command shows IPv6 FIB entries:

```
ACOS(config)#show ipv6 fib
Prefix                        Next Hop        Interface
Metric     Index
-------------------------------------------------------------------
--------------
b101::/64                     ::              Ethernet 6
256        0
Total routes = 1
```

show ip fragmentation

Description Show statistics for IP fragmentation or IPv6 fragmantation or IPv4-in-IPv6 fragmantation or IPv6-in-IPv4 fragmantation.

Syntax

```
show {ip | ipv6 | ipv4-in-ipv6 | ipv6-in-ipv4}
fragmentation statistics
```

Mode All

Example Example output for this command:

```
ACOS(config)#show ip fragmentation statistics
IP Fragmentation Statistics
---------------------------
Session Inserted                          0
Session Expired                           0
ICMP Received                             0
ICMPv6 Received                           0
UDP Received                              0
TCP Received                              0
```

```
IP-in-IP Received                          0
IPv6-in-IP Received                        0
Other Received                             0
ICMP Dropped                               0
ICMPv6 Dropped                             0
UDP Dropped                                0
TCP Dropped                                0
IP-in-IP Dropped                           0
IPv6-in-IP Dropped                         0
Other Dropped                              0
Overlapping Fragment Drop                  0
Bad IP Length                              0
Fragment Too Small Drop                    0
First TCP Fragment Too Small Drop          0
First L4 Fragment Too Small Drop           0
Total Sessions Exceeded Drop               0
Out of Session Memory                      0
Fragmentation Fast Aging Set               0
Fragmentation Fast Aging Unset             0
Fragment Queue Success                     0
Payload Length Unaligned                   0
Payload Length Out of Bounds               0
Duplicate First Fragment                   0
Duplicate Last Fragment                    0
Total Queued Fragments Exceeded            0
Fragment Queue Failure                     0
Fragment Reassembly Success                0
Fragment Max Data Length Exceeded          0
Fragment Reassembly Failure                0
MTU Exceeded Policy Drop                   0
Fragment Processing Drop                   0
Too Many Packets Per Reassembly Drop       0
Session Max Packets Exceeded               0
```

The following table describes the fields in the command output.

Field	Description
Session Inserted	Number of times the ACOS Device received a new fragment that did not match any existing session

Field	Description
	(based on source IP, destination ID, and fragment ID). A fragment session represents multiple fragments that should be reassembled together into a single logical packet.
Session Expired	Number of times a fragment session timed out before all the fragments for the packet were received.
ICMP Received	Number of ICMP fragments received.
ICMPv6 Received	Number of ICMPv6 fragments received.
UDP Received	Number of UDP fragments received.
TCP Received	Number of TCP fragments received.
IP-in-IP Received	Number of IP-in-IP fragments received.
IPv6-in-IP Received	Number of IPv6-in-IP fragments received.
Other Received	Number of other types of fragments received.
ICMP Dropped	Number of ICMP fragments that were dropped. This counter and the other “Dropped” counters below are incremented when a fragment is dropped for any of the following reasons: • Invalid length • Overlap with other fragments • Exceeded fragmentation session threshold
ICMPv6 Dropped	Number of ICMPv6 fragments that were dropped.
UDP Dropped	Number of UDP fragments that were dropped.
TCP Dropped	Number of TCP fragments that were dropped.

Field	Description
IP-in-IP Dropped	Number of IP-in-IP fragments that were dropped.
IPv6-in-IP Dropped	Number of IPv6-in-IP fragments that were dropped.
Other Dropped	Number of other types of fragments that were dropped.
Overlapping Fragment Drop	Number of fragments dropped because the data in the fragment overlapped with data in another fragment already received by the ACOS Device.
Bad IP Length	This counter includes both of the following: Number of IPv4 packets for which the total length was invalid. Number of IPv6 packets for which the payload length was invalid.
Fragment Too Small Drop	Number of fragments in which the length of the data was too short. IP fragmentation requires at least 8 bytes of data in all except the last fragment.
First TCP Fragment Too Small Drop	Number of fragmented TCP packets that did not contain the entire Layer 4 header in the first fragment.
First L4 Fragment Too Small Drop	Number of fragmented packets other than TCP packets that did not contain the entire Layer 4 header in the first fragment.
Total Sessions Exceeded Drop	Number of times a fragment was dropped because the maximum number of concurrent fragment sessions were already in use.
Out of Session Memory	Number of times the ACOS Device ran out of memory for fragment sessions.
Fragmentation Fast Aging Set	Number of times the ACOS Device sped up aging of existing fragment sessions in order to accommodate new sessions.

Field	Description
Fragmentation Fast Aging Unset	Number of times the ACOS Device returned to normal aging for fragment sessions.
Fragment Queue Success	Number of times a new fragment session was created, or a new fragment was added to an existing session.
Payload Length Unaligned	Number of fragments whose length did not consist of a multiple of 8 bytes. **NOTE:** This counter does not apply to the final fragments of fragmented packets. The final fragment of a packet is not required to have a length that is a multiple of 8.
Payload Length Out of Bounds	Number of times a fragmented packet's data length exceeded what should have been the end of the reassembled packet.
Duplicate First Fragment	Number of times a duplicate first fragment was received for the same packet.
Duplicate Last Fragment	Number of times a duplicate last fragment was received for the same packet.
Total Queued Fragments Exceeded	Number of times the maximum number of concurrent fragmented packets supported by the ACOS Device was exceeded.
Fragment Queue Failure	Total number of times a fragmented packet could not be queued to a session, due to any of the errors listed separately by the following counters: • Duplicate First Fragment • Duplicate Last Fragment • Payload Length Out of Bounds • Payload Length Unaligned
Fragment	Number of times all fragments for a packet were

Field	Description
Reassembly Success	reassembled successfully.
Fragment Max Data Length Exceeded	Number of times the total length of all reassembled fragments for a packet exceeded 65535. This type of error can indicate an attack such as a ping-of-death attack.
Fragment Reassembly Failure	Total number of fragment reassembly errors, including errors due to unlikely causes such as memory corruption.
MTU Exceeded Policy Drop	Number of packets dropped due to an MTU exceeded policy.
Fragment Processing Drop	Number of packets dropped due to errors during fragment processing.
Too Many Packets Per Reassembly Drop	Number of packets dropped because too many fragments were received for the packet.
Session Max Packets Exceeded	Number of times the limit for fragmented packets has been reached.
IPv4-in-IPv6 Fragmentation Statistics (Not shown in the example above.)	These are the same as the counters described above, but they apply to packets fragmented into IPv4 fragments before being sent in the IPv6 tunnel. For example, these counters can apply to fragmented DS-Lite traffic. These counters are displayed if you use the **ipv6** option instead of the **ip** option.

show ip helper-address

Description Display DHCP relay information.

Syntax `show ip helper-address [detail]`

Mode All

Example The following command shows summary DHCP relay information:

```
ACOS(config)#show ip helper-address
Interface  Helper-Address            RX             TX       No-
Relay         Drops
---------  --------------  ------------  ------------  -------
-----  ------------
eth1       100.100.100.1               0              0
   0              0
ve5        100.100.100.1            1669           1668
   0              1
ve7                                 1668           1668
   0              0
ve8        100.100.100.1               0              0
   0              0
ve9        20.20.20.102                0              0
   0              0
```

The following table describes the fields in the command output.

Field	Description
Interface	ACOS interface. Interfaces appear in the output in either of the following cases: • A helper address is configured on the interface. • DHCP packets are sent or received on the interface.
Helper-Address	Helper address configured on the interface.
RX	Number of DHCP packets received on the interface.
TX	Number of DHCP packets sent on the interface.
No-Relay	Number of packets that were examined for DHCP relay but were not relayed, and instead received regular Layer 2/3 processing. Generally, this counter increments in the following cases:

Field	Description
	• DHCP packets are received on an interface that does not have a helper address and the packets are not destined to the relay. • DHCP packets are received on an interface that does have a helper address, but the packets are unicast directly from the client to the server and do not need relay intervention.
Drops	Number of packets that were ineligible for relay and were dropped.

Example The following command shows detailed DHCP relay information:

```
ACOS#show ip helper-address detail
IP Interface: eth1
------------
  Helper-Address: 100.100.100.1
  Packets:
            RX: 0
               BootRequest Packets : 0
               BootReply Packets   : 0
            TX: 0
               BootRequest Packets : 0
               BootReply Packets   : 0
  No-Relay: 0
  Drops:
            Invalid BOOTP Port  : 0
            Invalid IP/UDP Len  : 0
            Invalid DHCP Oper   : 0
            Exceeded DHCP Hops  : 0
            Invalid Dest IP     : 0
            Exceeded TTL        : 0
            No Route to Dest    : 0
            Dest Processing Err : 0

IP Interface: ve5
------------
  Helper-Address: 100.100.100.1
  Packets:
```

```
            RX: 16
               BootRequest Packets : 16
               BootReply Packets   : 0
            TX: 14
               BootRequest Packets : 0
               BootReply Packets   : 14
  No-Relay: 0
  Drops:
            Invalid BOOTP Port  : 0
            Invalid IP/UDP Len  : 0
            Invalid DHCP Oper   : 0
            Exceeded DHCP Hops  : 0
            Invalid Dest IP     : 0
            Exceeded TTL        : 0
            No Route to Dest    : 2
            Dest Processing Err : 0

IP Interface: ve7
------------
  Helper-Address: None
  Packets:
            RX: 14
               BootRequest Packets : 0
               BootReply Packets   : 14
            TX: 14
               BootRequest Packets : 14
               BootReply Packets   : 0
  No-Relay: 0
  Drops:
            Invalid BOOTP Port  : 0
            Invalid IP/UDP Len  : 0
            Invalid DHCP Oper   : 0
            Exceeded DHCP Hops  : 0
            Invalid Dest IP     : 0
            Exceeded TTL        : 0
            No Route to Dest    : 0
            Dest Processing Err : 0
```

The following table describes the fields in the command output.

Field	Description
IP Interface	ACOS interface.
Helper-Address	IP address configured on the ACOS interface as the DHCP helper address.
Packets	DHCP packet statistics: • RX – Total number of DHCP packets received on the interface. • BootRequest Packets – Number of DHCP boot request packets (Op = BOOTREQUEST) received on the interface. • BootReply Packets – Number of DHCP boot reply packets (Op = BOOTREPLY) received on the interface. • TX – Total number of DHCP packets sent on the interface. • BootRequest Packets – Number of DHCP boot request packets (Op = BOOTREQUEST) sent on the interface. • BootReply Packets – Number of DHCP boot reply packets (Op = BOOTREPLY) sent on the interface.
No-Relay	Number of packets that were examined for DHCP relay but were not relayed, and instead received regular Layer 2/3 processing. Generally, this counter increments in the following cases: • DHCP packets are received on an interface that does not have a helper address and the packets are not destined to the relay. • DHCP packets are received on an interface that does have a helper address, but the packets are unicast

Field	Description
	directly from the client to the server and do not need relay intervention.
Drops	Lists the following counters for packets dropped on the interface: • Invalid BOOTP Port – Number of packets dropped because they had UDP destination port 68 (BOOTPC). • Invalid IP/UDP Len – Number of packets dropped because the IP or UDP length of the packet was shorter than the minimum required length for DHCP headers. • Invalid DHCP Oper – Number of packets dropped because the Op field in the packet header did not contain BOOTREQUEST or BOOTREPLY. • Exceeded DHCP Hops – Number of packets dropped because the number in the Hops field was higher than 16. • Invalid Dest IP – Number of packets dropped because the destination was invalid for relay. • Exceeded TTL – Number of packets dropped because the TTL value was too low (less than or equal to 1). • No Route to Dest – Number of packets dropped because the relay agent (ACOS Device) did not have a valid forwarding entry towards the destination. • Dest Processing Err – Number of packets dropped because the relay agent experienced an error in sending the packet towards the destination.

show ip interfaces | show ipv6 interfaces

Description Display IP interfaces.

Syntax

```
show {ip | ipv6} interfaces
[ethernet num] |
```

```
[ve num] |
[loopback num] |
[management] |
[trunk [num]] |
[lif [num]]
```

Mode All

Example The following command shows the IPv4 interfaces configured on Ethernet interface 1:

```
ACOS#show ip interfaces ethernet 1
IP addresses on ethernet 1:
  ip 10.10.10.241 netmask 255.255.255.0 (Primary)
  ip 10.10.10.242 netmask 255.255.255.0
  ip 10.10.10.243 netmask 255.255.255.0
  ip 10.10.10.244 netmask 255.255.255.0
  ip 10.10.11.244 netmask 255.255.255.0
```

Example The following command shows the IPv4 interfaces configured on VEs:

```
ACOS#show ip interfaces ve
Port IP              Netmask         PrimaryIP
-------------------------------------------------
-------------------------------------------------
ve4  60.60.60.241    255.255.255.0   Yes
     50.60.60.241    255.255.252.0   No
-------------------------------------------------
ve6  99.99.99.241    255.255.255.0   Yes
```

The PrimaryIP column indicates whether the address is the primary IP address for the interface.

Related Commands:

- ip address

show ip nat alg pptp

Description Display Application Level Gateway (ALG) information for IP source NAT.

Syntax

```
show ip nat alg pptp {statistics | status}
```

Example The following command displays the status of the PPTP NAT ALG feature:

```
ACOS#show ip nat alg pptp status
NAT ALG for PPTP is enabled on port 1723.
```

Example The following command displays PPTP NAT ALG statistics.

```
ACOS(config-if:ethernet:2)#show ip nat alg pptp statistics
Statistics for PPTP NAT ALG:
----------------------------
Calls In Progress:                  10
Call Creation Failure:              0
Truncated PNS Message:              0
Truncated PAC Message:              0
Mismatched PNS Call ID:             1
Mismatched PAC Call ID:             0
Retransmitted PAC Message:          3
Truncated GRE Packets:              0
Unknown GRE Packets:                0
No Matching GRE Session:          4
```

The following table describes the fields in the command output.

Field	Description
Calls In Progress	Current call attempts, counted by inspecting the TCP control session. This counter will decrease once the first GRE packet arrives.
Call Creation Failure	Number of times a call could not be set up because the ACOS Device ran out of memory or other system resources.
Truncated PNS Message	Number of runt TCP PPTP messages received from clients.
Truncated PAC Message	Number of runt TCP PPTP messages received from servers.
Mismatched PNS Call ID	Number of calls that were disconnected because the GRE session had the wrong Call ID.

Field	Description
Mismatched PAC Call ID	Number of calls that were disconnected because they had the wrong Call ID.
Retransmitted PAC Message	Number of TCP packets retransmitted from PAC servers.
Truncated GRE Packets	Number of runt GRE packets received by the ACOS Device.
Unknown GRE Packets	Number of GRE packets that were not used for PPTP and were dropped.
No Matching GRE Session	Number of GRE PPTP packets sent with no current call.

show ip nat interfaces | show ipv6 nat interfaces

Description Display IP or IPv6 source NAT information for data interfaces.

Syntax

```
show {ip | ipv6} nat interfaces
```

Example The following command shows the IP NAT interface settings:

```
ACOS#show ip nat interfaces
Total IP NAT Interfaces configured: 2
Interface       NAT Direction
-----------------------------
ve10            outside
ve11            inside
```

show ip isis | show ipv6 isis

Description Display ISIS information.

show ip nat pool | show ipv6 nat pool

Description Display information for IP or IPv6 source NAT pools.

Syntax

```
show {ip | ipv6} nat pool [pool-name] [statistics]
```

Parameter	Description
pool-name	Displays information only for the specified pool.
statistics	Displays pool statistics.

Example The following command displays pool information:

```
ACOS#show ip nat pool
Total IP NAT Pools: 2
Pool Name             Start Address    End Address      Mask
Gateway          Vrid
-------------------------------------------------------------------
---------------------------
dmz1                  10.0.0.200       10.0.0.200       /24
0.0.0.0          default
dmz2                  10.10.10.200     10.10.10.200     /24
0.0.0.0          default
```

The following table describes the fields in the command output.

Field	Description
Pool Name	Name of the pool.
Start Address	Beginning IP address in the pool address range.
End Address	Ending IP address in the pool address range.
Mask	Network mask.
Gateway	Default gateway for traffic mapped to an address in the pool.
Vrid	VRRP-A VRID to which the pool is assigned, if applicable.

```
Entering a pool name displays the same fields but for only the
specified pool:
ACOS#show ip nat pool dmz1
Pool Name             Start Address    End Address      Mask
Gateway          Vrid
-------------------------------------------------------------------
---------------------------------
```

```
dmz1                    10.0.0.200        10.0.0.200        /24
0.0.0.0          default
```

Example The following command displays pool statistics:

```
ACOS#show ip nat pool statistics
Pool          Address           Port Usage   Total Used   Total
Freed  Failed
-------------------------------------------------------------------
-----------------
dmz1          10.0.0.200        0            0            0
      0
Pool          Address           Port Usage   Total Used   Total
Freed  Failed
-------------------------------------------------------------------
-----------------
dmz2          10.10.10.200      0            0            0
      0
```

The following table describes the fields in the command output.

Field	Description
Pool	Name of the pool.
Address	IP address in the pool.
Port Usage	Number of Layer 4 protocol port mappings currently in use on the port. **NOTE:** A local address can have multiple NAT mappings. Each NAT mapping for a local address consists of an IP:port tuple.
Total Used	Total number of port mappings (IP:port tuples) used from the pool.
Total Freed	Total number of port mappings that were used and then returned to the pool.
Failed	Number of mappings that failed.

show ip nat pool-group | show ipv6 nat pool-group

Description Display configuration information for IP or IPv6 source NAT pool groups.

Syntax

```
show {ip | ipv6} nat pool-group [group-name]
```

show ip nat range-list

Description Displays information for IP source NAT range lists.

Syntax

```
show ip nat range-list
```

Example The following command shows NAT range-list information:

```
ACOS(config)#show ip nat range-list
Total Static NAT range lists: 1
Name             Local Address/Mask           Global
Address/Mask          Count HA
------------------------------------------------------------------
------------------
rl1              10.10.10.88/24               192.168.10.88/24
           10     0
```

The following table describes the fields in the command's output.

Field	Description
Name	Name of the range list.
Local Address/Mask	Beginning local address of the range to be translated into global (NAT) addresses.
Global Address/Mask	Beginning global address of the range.
Count	Number of address translations in the range.
HA	VRRP-A VRID to which the range list belongs, if applicable.

show ip nat static-binding

Description Display information for static IP source NAT bindings.

Syntax

```
show ip nat static-binding [statistics] [ipaddr]
```

Parameter	Description
statistics	Displays statistics.
ipaddr	Displays information for the specified IP address.

Example The following command displays the static source NAT binding for local address 10.10.10.20:

```
ACOS#show ip nat static-binding 10.10.10.20
Local Address 10.10.10.20 statically bound to Global Address
10.10.10.1
```

Example The following command displays static-binding statistics:

```
ACOS#show ip nat static-binding statistics
Source Address        Port Usage    Total Used    Total Freed
-------------------------------------------------------------
-------------
10.10.10.20           0             0             0
```

The following table describes the fields in the command output.

Field	Description
Source Address	Source IP address that is statically mapped to a global IP address (source NAT address).
Port Usage	Number of Layer 4 protocol port mappings currently in use by the local address. **NOTE:** A local address can have multiple NAT mappings. Each NAT mapping for a local address consists of an IP:port tuple.
Total Used	Total number of port mappings (IP:port tuples) used by the inside address.

Field	Description
Total Freed	Total number of port mappings returned to the static pool.

show ip nat statistics

Description Displays IP source NAT statistics.

Syntax

```
show ip nat statistics
```

Example Displays IP NAT statistics:

```
ACOS(config)#show ip nat statistics
Outside interfaces: ethernet8, ethernet11, ve20, ve110, ve120
Inside interfaces:  ethernet8, ethernet11, ve20, ve110, ve120
Hits: 1707  Misses: 0
Outbound TCP sessions created: 1363
Outbound  UDP sessions created: 344
Outbound  ICMP sessions created: 0
Inbound  TCP sessions created: 0
Inbound  UDP sessions created: 0
Dynamic mappings:
-- Inside Source
access-list 8 pool v4
start 10.10.120.200 end 10.10.120.202
total addresses 3, allocated 2315, misses 0
access-list v6 pool l3nat6
start 6020::203 end 6020::203
total addresses 1, allocated 0, misses 0
```

The output lists the inside NAT and outside NAT interfaces and provides address translation statistics.

show ip nat template logging

Description Display configuration information for IP source NAT logging templates.

Syntax

```
show ip nat template logging [template-name]
```

show ip nat timeouts

Description Display the IP source NAT protocol port timeouts.

Syntax

```
show ip nat timeouts
```

Example The following command displays the timeout settings IP source NAT sessions.

```
ACOS(config)#show ip nat timeouts
NAT Timeout values in seconds:
TCP    UDP    ICMP
------------------------
300    300    fast
Service 53/udphas fast-aging configured
```

show ip nat translations

Description Display IP source NAT translations.

Syntax

```
show ip nat translations
```

Mode All

Example The following command shows source NAT translations:

```
ACOS#show ip nat translations
Prot Inside global          Inside local           Outside
local          Outside global         Age Hash Type
------------------------------------------------------------------
-------------------------------------------------
Tcp  10.10.120.200:33345      10.10.30.19:35955
10.10.120.124:1107       10.10.120.124:1107       0      1
NF NAT
Tcp  10.10.120.200:28260      10.10.30.16:64602
10.10.120.111:443        10.10.120.111:443        0      1
NS NAT
Tcp  10.10.120.200:29988      10.10.30.20:2466
10.10.120.111:80         10.10.120.111:80         0      1
NS NAT
```

```
Tcp  10.10.120.200:29952      10.10.30.16:64638
10.10.120.124:21          10.10.120.124:21          0       1
NS NAT
Tcp  10.10.120.200:9257       10.10.30.15:48569
10.10.120.124:1093        10.10.120.124:1093        0       1
NF NAT
Tcp  10.10.120.200:28170      10.10.30.18:38106
10.10.120.124:21          10.10.120.124:21          0       1
NS NAT
Tcp  10.10.120.200:29845      10.10.30.15:48619
10.10.120.111:443         10.10.120.111:443         0       2
NS NAT
Tcp  10.10.120.200:28716      10.10.30.15:48624
10.10.120.124:1111        10.10.120.124:1111        0       2
NF NAT
Tcp  10.10.120.200:29377      10.10.30.19:35947
10.10.120.111:80          10.10.120.111:80          0       2
NS NAT
Tcp  10.10.120.200:29179      10.10.30.15:48565
10.10.120.111:443         10.10.120.111:443         0       2
NS NAT
Tcp  10.10.120.200:21887      10.10.30.15:48635
10.10.120.124:1118        10.10.120.124:1118        0       2
NF NAT
Tcp  10.10.120.200:21800      10.10.30.18:38108
10.10.120.124:1097        10.10.120.124:1097        0       2
NF NAT
Tcp  10.10.120.200:29971      10.10.30.20:2467
10.10.120.111:443         10.10.120.111:443         0       2
NS NAT
```

The following table describes the fields in the command's output.

Field	Description
Prot	Layer 4 protocol.
Inside global	Global (NAT) address mapped by ACOS to the inside source address (the inside local address).

Field	Description
Inside local	Inside source address before translation.
Outside local	Outside destination address of the traffic.
Outside global	Outside destination address of the traffic.
Age	For dynamic mappings, indicates how many seconds the entry is allowed to continue remaining idle before being removed.

show ip ospf | show ipv6 ospf

Description Display OSPF information.

show ip prefix-list | show ipv6 prefix-list

Description Display information about prefix lists.

Syntax

```
show {ip | ipv6} prefix-list
```

Mode All

show ip protocols | show ipv6 protocols

Description Show information for dynamic routing protocols.

Syntax

```
show {ip | ipv6} protocols
```

Mode All

show ip rip | show ipv6 rip

Description Show information for RIP.

show ip route | show ipv6 route

Description Displays the IPv4 or IPv6 routing table.

Syntax

```
show {ip | ipv6} route
[
ipaddr[/mask-length] |
all |
bgp |
connected |
database |
isis |
mgmt |
ospf |
rip |
static |
summary
]
```

Mode All

Usage The **all** option is only applicable for IPv4.

The **show ip route summary** command displays summary information for all IP routes, including the total number of routes. The command output applies to both the data route table and the management route table, which are separate route tables.

The following commands display routes for only one of the route tables:

- **show ip route** – Shows information for the data route table only.
- **show ip route mgmt** – Shows information for the management route table only.

The total number of routes listed by the output differs depending on the command you use. For example, the total number of routes listed by the **show ip route** command includes only data routes, whereas the total number of routes listed by the **show ip route summary** command includes data routes *and* management routes.

Example The following example shows the IP route table:

```
ACOS#show ip route
Codes: C - connected, S - static, O - OSPF
```

```
S*    0.0.0.0/0 [1/0] via 192.168.20.1, ve 10
S*    192.168.1.0/24 [1/0] is directly connected, Management
C*    192.168.1.0/24 is directly connected, Management
C*    192.168.19.0/24 is directly connected, ve 10
Total number of routes : 4
```

Example The following example shows the ip route mgmt. The second management (management2) details are displayed only for the Thunder 8665S platform:

```
ACOS#show ip route mgmt
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default

Gateway of last resort is 10.65.28.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.65.28.1, management2, 00:00:00
[1/0] via 10.65.21.1, management, 00:00:00
C     10.65.21.0/24 is directly connected, management,
00:00:40
C     10.65.28.0/24 is directly connected, management2,
01:22:04
S     192.168.20.1/24 [254/0] is directly connected, a10if0,
00:00:00
```

show ip stats | show ipv6 stats

Description View statistics for IPv4 or IPv6 packets.

Syntax

```
show {ip | ipv6} stats
```

Mode All

show ip-list

Description Display IP-list information.

Syntax

```
show ip-list [list-name]
```

Parameter	Description
list-name	Displays the configuration of the specified list. If you omit this option, the configured IP lists are listed instead.

Mode All

Example The following example shows the IP lists configured on an ACOS Device:

```
ACOS-Active(config)#show ip-list
Name                                Type      Entries
-------------------------------------------------------
sample_ip_list_ng                   IPv4      3
test-list                           IPv4      0
Total: 2
```

The following command shows the configuration of an individual IP list:

```
ACOS#show ip-list sample_ip_list_ng
ip-list sample_ip_list_ng
 10.10.10.1
 20.20.3.1
 123.45.6.7
```

show ipv6 ndisc

Description Display information for IPv6 router discovery.

Syntax

```
show ipv6 ndisc router-advertisement
{ethernet portnum | ve ve-num | statistics}
```

Mode All

Example

The following command displays configuration information for IPv6 router discovery on an Ethernet interface. In this example, the interface is VE 10.

```
ACOS#show ipv6 ndisc router-advertisement ve 10
Interface VE 10
Send Advertisements:                  Enabled
Max Advertisement Interval:           200
Min Advertisement Interval:           150
Advertise Link MTU:                   Disabled
Reachable Time:                       0
Retransmit Timer:                     0
Current Hop Limit:                    255
Default Lifetime:                     200
Max Router Solicitations Per Second: 100000
HA Group ID:                          None
Number of Advertised Prefixes:        2
 Prefix 1:
     Prefix:         2001:a::/96
     On-Link:        True
     Valid Lifetime: 4400
 Prefix 2:
     Prefix:         2001:32::/64
     On-Link:        True
     Valid Lifetime: 2592000
```

The following command displays router discovery statistics:

```
ACOS(config)#show ipv6 ndisc router-advertisement statistics
IPv6 Router Advertisement/Solicitation Statistics:
-------------------------------------------------
Good Router Solicitations (R.S.) Received:          1320
Periodic Router Advertisements (R.A.) Sent:         880
R.S. Rate Limited:                                  2
R.S. Bad Hop Limit:                                 1
R.S. Truncated:                                     0
R.S. Bad ICMPv6 Checksum:                           0
R.S. Unknown ICMPv6 Code:                           0
R.S. Bad ICMPv6 Option:                             0
R.S. Src Link-Layer Option and Unspecified Address: 0
No Free Buffers to send R.A.:                       0
```

The error counters apply to router solicitations (R.S.) that are dropped by the ACOS Device.

The Src Link-Layer Option and Unspecified Address counter indicates the number of times the ACOS Device received a router solicitation with source address "::" (unspecified IPv6 address) and with the source link-layer (MAC address) option set.

NOTE: In the current release, the ACOS Device does not drop ICMPv6 packets that have bad (invalid) checksums.

show ipv6 neighbor

Description Display information about neighboring IPv6 devices.

Syntax `show ipv6 neighbor [ipv6-address]`

Mode All

Example The following command shows IPv6 neighbors:

```
ACOS(config)#show ipv6 neighbor
Total IPv6 neighbor entries: 1
IPv6 Address              MAC Address    Type    Age  State
 Interface   Vlan/Encap
-----------------------------------------------------------------
-----------------------------------
6060::100                 021F.A000.00F8 Dynamic 201  Reachable
 lif 100           1
fe80::21f:a0ff:fe0f:bb82 001F.A00F.BB82 Dynamic 209  Stale
 Management        1
3010::1                   001F.A040.873C Dynamic 83   Reachable
 ve10              10
2020::100                 9EE2.C491.C75A Dynamic 82   Reachable
 ve20              20
```

The following table describes the fields in the command output.

Field	Description
Total IPv6 neighbor entries	The total number of IPv6 neighbor devices.
IPv6 Address	IPv6 address of the device.
MAC Address	MAC address of the device.
Type	Indicates whether the entry is static or dynamic.
Age	Number of seconds since the entry was last used in the dynamic entries.
Interface	ACOS interface through which the device that has the displayed MAC address and IPv6 address can be reached.
Vlan/Encap	VLAN or encapsulated tunnel through which the device that has the MAC address can be reached.

show ipv6 traffic

Description Display IPv6 traffic management statistics.

Syntax

```
show ipv6 traffic
```

Mode All

Example The following command shows IPv6 traffic management statistics:

```
ACOS#show ipv6 traffic
Traffic Type      Received        Sent            Errors
------------------------------------------------------------
----
Router Solicit    1               1               0
Router Adverts    0               0               0
Neigh Solicit     0               0               0
Neigh Adverts     0               0               0
Echo Request      0               0               0
Echo Replies      0               0               0
```

```
Other ICMPv6 Errs 0                0                0
```

show isis

Description Display ISIS information.

show json-config

Description View the JSON/aXAPI data format associated with the running-config, or for a specific object.

Syntax

```
show json-config [object]
```

If no *object* is specified, then the JSON configuration for the entire running-config will be shown.

Mode All

Example The following example shows the JSON configuration for SLB server “web2”:

```
ACOS#show json-config slb server web2

a10-url:/axapi/v3/slb/server/web2
{
  "server": {
    "name":"web2",
    "host":"10.10.10.2",
    "health-check":"https-with-key",
    "port-list": [
      {
        "port-number":80,
        "protocol":"tcp",
        "health-check-disable":1
      }
    ]
  }
}
```

Related Commands:

- show json-config-detail
- show json-config-with-default

show json-config-detail

Description View the JSON/aXAPI data format, including the URI and object type, associated with the running-config, or for a specific object.

Syntax

```
show json-config-detail [object]
```

If no *object* is specified, then the JSON configuration for the entire running-config will be shown.

Mode All

Example The following example shows the JSON configuration, with URI and object type information, for SLB server “web2”:

```
ACOS#show json-config-detail slb server web2

a10-url:/axapi/v3/slb/server/web2
{
  "server": {
    "name":"web2",
    "host":"10.10.10.2",
    "health-check":"https-with-key",
    "port-list": [
      {
        "port-number":80,
        "protocol":"tcp",
        "health-check-disable":1,
        "a10-url":"/axapi/v3/slb/server/web2/port/80+tcp",
        "obj-type":"multi"
      }
    ]
  }
}
```

Related Commands:

- show json-config

- show json-config-with-default

show json-config-with-default

Description View the JSON/aXAPI data format, including default values, associated with the running-config or for a specific object.

Syntax

```
show json-config-with-default [object]
```

If no *object* is specified, then the JSON configuration for the entire running-config will be shown.

Mode All

Example The following example shows the JSON configuration, with default values, for SLB server “web2”:

```
ACOS#show json-config-with-default slb server web2

a10-url:/axapi/v3/slb/server/web2
{
  "server": {
    "name":"web2",
    "host":"10.10.10.2",
    "action":"enable",
    "template-server":"default",
    "health-check":"https-with-key",
    "conn-limit":8000000,
    "no-logging":0,
    "weight":1,
    "slow-start":0,
    "spoofing-cache":0,
    "stats-data-action":"stats-data-enable",
    "extended-stats":0,
    "port-list": [
      {
        "port-number":80,
        "protocol":"tcp",
        "range":0,
        "action":"enable",
        "no-ssl":0,
```

```
        "health-check-disable":1,
        "weight":1,
        "conn-limit":8000000,
        "no-logging":0,
        "stats-data-action":"stats-data-enable",
        "extended-stats":0,
        "a10-url":"/axapi/v3/slb/server/web2/port/80+tcp"
      }
    ]
  }
}
```


Related Commands:

- show json-config
- show json-config-detail

show key-chain

Description Show configuration information for authentication key chains.

Syntax

```
show key-chain [key-chain-name]
```

The *key-chain-name* is the name of the authentication key chain.

Mode Privileged EXEC and all Config levels

Example The following text is an example of the output for this command:

```
ACOS#show key-chain
key chain test1
    key 1
                key-string test1key1
    key 2
            key-string test1key2
key chain test2
    key 2
             key-string test2key2


ACOS#show key-chain test1
key chain test1
   key 1
             key-string test1key1
   key 2
             key-string test1key2
```

show lacp

Description Show configuration information and statistics for Link Aggregation Control Protocol (LACP).

Syntax

```
show lacp
{
  counter [lacp-trunk-id] |
  sys-id |
  trunk
    [admin-key-list-details | detail | summary | lacp-trunk-id]
}
```

Parameter	Description
counter	View LACP packet statistics for all trunks, or for just the specified trunk.
sys-id	Shows the LACP system ID of the ACOS Device.
admin-key-list-details	View LACP admin key list details.

Parameter	Description
detail	View detailed trunk information.
summary	View trunk summary information.

Mode All

Example The following command shows LACP statistics:

```
ACOS#show lacp counters
 Traffic statistics
Port          LACPDUs          Marker          Pckt err
            Sent    Recv    Sent    Recv    Sent    Recv
 Aggregator po5 1000000
ethernet 1   81       81       0       0       0       0
ethernet 2   81       81       0       0       0       0
 Aggregator po10 1000001
ethernet 6   233767   233765   0       0       0       0
```

In this example, LACP has dynamically created two trunks, 5 and 10. Trunk 5 contains ports 1 and 2. Trunk 10 contains port 6.

Example The following command shows summary trunk information:

```
ACOS#show lacp trunk summary
 Aggregator po5 1000000
  Admin Key: 0005 - Oper Key 0005
   Link: ethernet 1 (3) sync: 1
   Link: ethernet 2 (4) sync: 1
 Aggregator po10 1000001
  Admin Key: 0010 - Oper Key 0010
   Link: ethernet 6 (8) sync: 1
```

show lacp-passthrough

Description Show information for the LACP passthrough feature.

Syntax

```
show lacp-passthrough
```

Mode All

show license

Description Display the host ID and, if applicable, serial number of the license applied to this ACOS Device.

Syntax

```
show license [uid]
```

Specify the **uid** option to show the serial number associated with the UID.

Mode Privileged EXEC or higher

Example The following example shows sample output for this command.

```
ACOS# show license
Host ID: 029984E1BC8EF50901B63DC0DCD1FE8A02017B9B
ACOS# show license uid
029984E1BC8EF50901B63DC0DCD1FE8A02017B9B
```

show license-debug

Description This command is for internal use and is documented to notify that it does not serve any useful purpose to the consumer.

Syntax

```
show license-debug
```

Mode All

Example Example output for this command:

```
ACOS> show license-debug
Host ID  : A0C764C33831F0A6FB9861EA6EDCF31330FB91A6
Product  : ADC
Platform : AX-V
-----------------------------------------------
 Source   Enabled Licenses         Expiry Date
-----------------------------------------------
BUILT IN
            SLB                   None
            CGN                   None
            GSLB                  None
```

```
            RC                          None
            DAF                         None
            WAF                         None

GLM
```

show license-info

Description Show current product SKU and license information on the ACOS Device.

Syntax

```
show license-info
```

Mode All

Example The following example shows that the CFW product is installed (highlighted) along with the product modules that are included in this product. Refer to the *Release Notes* for more information about product SKUs and licenses.

```
ACOS> show license-info
Host ID  : 5DCB01EC264BECCCFECB3C2ED42E02384EE8C527
Product  : CFW
Platform : AX Series Advanced Traffic Manager
GLM Ping Interval In Hours : 24
------------------------------------------------------------------
----------------------
Enabled Licenses          Expiry Date
Notes
------------------------------------------------------------------
----------------------
SLB                       None
CGN                       None
GSLB                      None
RC                        None
DAF                       None
WAF                       None
SSLI                      None
DCFW                      None
GIFW                      None
```

```
URLF                        None
IPSEC                       None
AAM                         None
FP                          None
WEBROOT                     None              Requires an
additional Webroot license.
THREATSTOP                  None              Requires an
additional ThreatSTOP license.
```

Example The following example displays the SSLI, DCFW, GIFW, ADC product licenses as well as the NGWAF pool license with the NGWAF bandwidth field in Mbps (available from ACOS 6.0.6 onwards).

```
AACOS(config)#show license-info
Host ID         : CXXXXAAXXXX2C932C241F3C4B30FXXXXXXXXXXXX
Serial No       : N/A
USB ID          : Not Available
Billing Serials: vTh906xxxxxxe0000, vThcxxxxxxxd0000
Token           : Not Available
Product         : ADC
Platform        : vThunder
Burst           : Disabled
Version         : N/A Green
GLM Ping Interval In Hours : 24
Product-description        : N/A
-------------------------------------------------------------
------------------
                  ----
Enabled Licenses            Expiry Date (UTC)
Notes
-------------------------------------------------------------
------------------
                  ----
SLB                         None
CGN                         None
GSLB                        None
RC                          None
DAF                         None
WAF                         None
SSLI                        22-December-2024
DCFW                        22-December-2024
```

```
GIFW                        22-December-2024
URLF                        22-December-2024
AAM                         None
FP                          None
WEBROOT                     None              License Type: No
webroot type found
THREATSTOP                  None
QOSMOS                      N/A               Requires an
additional QOSMOS license
                           .
WEBROOT_TI                  N/A               Requires an
additional Webroot Threat
                            Intel license.
IPSEC_VPN                   N/A               Requires an
additional IPsec VPN lice
                           nse.
A10_TI                      N/A               Requires an
additional A10 Threat Int
                           el license.
SECURE_GAMING               N/A               Requires an
additional Secure gaming
                           license.
PRIVILEGE_SHELL_ROOT        N/A               Requires an
additional Privilege shel
                           l root license.
NGWAF                       10-May-2025
5 Mbps Bandwidth            22-December-2024
10 NGWAF Mbps BW (E)        10-May-2025
```

show lldp neighbor statistics

Description Displays information on all remote neighbors or on the specified interface.

Syntax **show lldp neighbor statistics** [**interface Ethernet** *eth-num*]

Mode All

show lldp statistics

Description Displays LLDP receive or send error statistics, You can display information on all interfaces or only display information on a specified interface.

Syntax

```
show lldp statistics
[interface {ethernet eth-num | management}]
```

Mode All

show locale

Description Display the configured CLI locale.

Syntax

```
show locale
```

Mode All

Example The following command shows the locale configured on an ACOS Device:

```
ACOS#show locale
  en_US.UTF-8    English locale for the USA, encoding with
UTF-8 (default)
```

show local-log database

Description Displays local log information. You can list all databases, statistics of local-log databases, or information for a specific database.

Syntax

```
show local-log database [all [limit] | stats | local-log-db-
name]
```

Mode All

show local-uri-file

Description Display local imported URI files.

Syntax

```
show local-uri-file
[name] [all-partitions] [partition {shared | partition-name}]
```

Mode All

show log

Description Display entries in the syslog buffer or display current log settings (policy). Log entries are listed starting with the most recent entry on top.

Note: The log format displayed in the **show log** depends on the configuration of the format in the **acos-events collector-group** command.

Syntax

```
show log [debug] [length  num] [policy]
```

Parameter	Description
debug	Show debug logging entries only.
length *num*	Shows the most recent log entries, up to the number of entries you specify. You can specify 1-1000000 (one million) entries.
policy	Shows the log settings. To display log entries, omit this option.

Mode All

Example The following command shows the log settings:

```
ACOS#show log policy
Syslog servers: (0 hosts)

Facility: local0

Name                Level
----------------------------
Console             error
Syslog              disable
Monitor             disable
Buffer              debugging
```

```
Email                disable
Trap                 disable
```

Example The following command shows log entries (truncated for brevity):

```
ACOS#show log
Log Buffer: 30000
Jan 17 11:32:02   Warning A10LB HTTP request has p-conn
Jan 17 11:31:01   Notice  The session [1] is closed
Jan 17 11:31:00   Info    Load libraries in 0.044 secs
Jan 17 11:26:19   Warning A10LB HTTP request has p-conn
Jan 17 11:26:19   Warning A10LB HTTP response not beginning of
header: m counterType="1" hourlyCount="2396"
dailyCount="16295" weeklyCount="16295" monthly
Jan 17 11:16:18   Warning A10LB HTTP request has p-conn
Jan 17 11:16:01   Notice  The session [1] is closed
Jan 17 11:16:00   Info    Load libraries in 0.055 secs
Jan 17 11:15:22   Warning A10LB HTTP request has p-conn
Jan 17 11:15:03   Notice  The session [1] is closed
Jan 17 11:14:33   Warning A10LB HTTP request has p-conn
...
```

show mac-address-table

Description Display MAC table entries.

Syntax

```
show mac-address-table
[macaddr | port port-num | vlan vlan-id]
```

Parameter	Description
macaddr	Shows the MAC table entry for the specified MAC address. Enter the MAC address in the following format: aaaa.bbbb.cccc
port *port-num*	Shows the MAC table entries for the specified Ethernet port.
vlan *vlan-id*	Shows the MAC table entries for the specified VLAN.

Mode All

Example The following command displays the MAC table entries:

```
ACOS#show mac-address-table
Total active entries: 10        Age time: 300 secs
MAC-Address      Port     Type      Index     Vlan  Trap
-----------------------------------------------------------
001e.bd62.d021   2        Dynamic   85        0     None
001e.bd62.d01e   1        Dynamic   244       120   None
000c.2923.c500   lif2     Dynamic   456       1     None
000d.480a.6665   1        Dynamic   594       120   None
001f.a002.fdc3   1        Dynamic   676       120   None
000c.2923.c500   2        Dynamic   713       60    None
001e.bd62.d01e   1        Dynamic   734       0     None
000c.2960.8990   1        Dynamic   752       120   None
001f.a002.10a8   5        Dynamic   918       100   None
001e.bd62.d021   2        Dynamic   975       60    None
```

The following table describes the fields in the command output.

Field	Description
Total active entries	Total number of active MAC entries in the table. An active entry is one that has not aged out.
Age time	Number of seconds a dynamic (learned) MAC entry can remain unused before it is removed from the table.
MAC-Address	MAC address of the entry.
Port	Ethernet port through which the MAC address is reached.
Type	Indicates whether the entry is dynamic or static.
Index	The MAC entry's position in the MAC table.
Vlan	VLAN the MAC address is on.
Trap	Shows any SNMP traps enabled on the port.

show management

Description Shows the types of management access allowed on each of the ACOS Device's Ethernet interfaces.

If management access is controlled by an ACL, the ACL ID is listed in place of "on" or "off" status.

Syntax

```
show management [ipv4 | ipv6]
```

Mode All

NOTE: If you do not use either option, IPv4 access information is shown.

Example The following command shows IPv4 management access information:

```
       PING      SSH     Telnet      HTTP       HTTPS
      SNMP      ACL
-------------------------------------------------------------------
----------------------------
mgmt    on        on       off         on         on
         on         -
eth1    on        off      off         off        off
        off        -
eth2    on        off      off         off        off
        off        -
eth3    on        off      off         off        off
        off        -
eth4    on        off      off         off        off
        off        -
...
```

Example The commands in the example below use an ACL to control telnet service on the management interface, then display the status with the show management command.

```
ACOS(config)# access-list 17 permit any
ACOS(config)# enable-management service telnet
ACOS(config-enable-management telnet)# acl-v4 17
ACOS(config-enable-management telnet-acl...)# management
```

```
ACOS(config-enable-management telnet-acl...)# show management

PING     SSH       Telnet    HTTP      HTTPS     SNMP      ACL
-------------------------------------------------------------
------
mgmt    on        on        ACL
17    on        on        on        -
eth1    on        off       off       off       off       off
     -
eth2    on        off       off       off       off       off
     -
eth3    on        off       off       off       off       off
     -
ACOS(config-enable-management telnet-acl...)#
```

Example The commands in the example below use an ACL to control all unconfigured services on the management interface, then display the status.

```
ACOS(config)# access-list 18 permit any
ACOS(config)# enable-management service acl-v4 18
ACOS(config-enable-management telnet-acl...)# show management
      PING     SSH     Telnet  HTTP    HTTPS   SNMP    ACL
-------------------------------------------------------------
mgmt  ACL 18   ACL 18  ACL 17  ACL 18  ACL 18  ACL 18  18
eth1  on       off     off     off     off     off     -
eth2  on       off     off     off     off     off     -
eth3  on       off     off     off     off     off     -
ACOS(config-enable-management telnet-acl...)#
```

Example The commands in the example below disable ACOS from responding to the NTP client requests on ethernet 3, then display the status with the `show management` command.

```
ACOS(config)# disable-management service ntp
ACOS(config-disable-management ntp)# ethernet 3
ACOS(config-disable-management ntp)# show management
        PING SSH   Telnet HTTP   HTTPS  SNMP   NTP  ACL
-------------------------------------------------------------
mgmt    on   on    off    on     on     on     on   -
eth1    on   off   off    off    off    off    on   -
```

```
eth2     on    off    off     off     off     off     on    -
eth3     on    off    off     off     off     off     off   -
eth4     on    off    off     off     off     off     on    -
eth5     on    off    off     off     off     off     on    -
eth6     on    off    off     off     off     off     on    -
ve110    on    off    off     off     off     off     on    -
ve210    on    off    off     off     off     off     on    -
ACOS(config-disable-management ntp)#
```

Example The commands in the example below configure an ACL on ethernet 3, then display the status with the `show management` command.

```
ACOS(config)# enable-management service acl-v4 1
ACOS(config-enable-management acl-v4)# ethernet 3
ACOS(config-enable-management acl-v4)# show management
         PING    SSH     Telnet   HTTP    HTTPS   SNMP    NTP    ACL
-----------------------------------------------------------------
------
mgmt     on      on      off      on      on      on      on
eth1     on      off     off      off     off     off     on     -
eth2     on      off     off      off     off     off     on     -
eth3     ACL 1   ACL 1   ACL 1    ACL 1   ACL 1   ACL 1   ACL 1  ACL 1
eth4     on      off     off      off     off     off     on     -
eth5     on      off     off      off     off     off     on     -
eth6     on      off     off      off     off     off     on     -
ve110    on      off     off      off     off     off     on     -
ve210    on      off     off      off     off     off     on     -
ACOS(config-enable-management ntp)#
```

Related Commands:

- enable-management
- disable-management

show memory

Description Display memory usage information.

Syntax

```
show memory [cache | system | active-vrid {vrid-num |
default}]
```

Parameter	Description
cache	Shows cache statistics.
system	Shows summary statistics for memory usage.
active-vrid	Show memory usage statistics for the specified VRID only. This option is only available in VRRP-A environments.

Mode Privileged EXEC level and configuration levels

Example The following command shows summary statistics for memory usage:

```
ACOS#show memory system
System Memory Usage:
Total(KB)  Free       Shared     Buffers    Cached     Usage
-----------------------------------------------------------------
-------------
2070368    751580     0          269560     96756      59.0%
```

Example The following command shows memory usage for individual system modules:

```
ACOS#show memory
Total(KB)  Used       Free       Usage
-------------------------------------------------
Memory:  31941112   8310060    23631052   26.0%
System memory:
Object size(byte)    Allocated(#)         Max(#)
-----------------------------------------------------------------
--
4                    223                  3639
36                   2536                 3639
100                  71095                71262
228                  152                  992
484                  12                   503
996                  183                  253
2020                 92                   127
4068                 339                  378
8164                 72                   93

aFleX memory:
```

```
Object size(byte)    Allocated(#)          Max(#)
-------------------------------------------------------------
--
32                   1412                  58224
64                   7008                  30816
128                  7621                  20960
256                  181                   12768
512                  509                   7168
1024                 52                    3824
2048                 0                     0
4096                 0                     0

TCP memory:
Object size(byte)    Allocated(#)          Max(#)
-------------------------------------------------------------
--
1104                 1                     225
184                  0                     0
```

Example The following command shows memory cache information (truncated for brevity):

```
ACOS#show memory cache
System block 4:
Object size: 4, Total in pool: 3639, Allocated to control: 223
Misc1 92 Misc2 1 Allocated to 16 data threads: 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

System block 36:
Object size: 36, Total in pool: 3639, Allocated to control:
2536
Misc1 0 Misc2 1 Allocated to 16 data threads: 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

System block 100:
Object size: 100, Total in pool: 71262, Allocated to control:
71095
Misc1 0 Misc2 37 Allocated to 16 data threads: 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
...
```

show mirror

Description Display port mirroring information.

Syntax

```
show mirror
```

Mode All

Example The following example shows the port mirroring configuration on an ACOS Device:

```
ACOS#show mirror
Mirror Ports 1:          Input = 4       Output = 4
 Ports monitored at ingress : 1
Mirror Ports 2:          Input = None    Output = 7
Mirror Ports 3:          Input = 9       Output = 9
Mirror Ports 4:          Input = 3       Output = None
```

The following table describes the fields in the command output.

Field	Description
Mirror Port	Mirror port index number.
Input	Indicates that inbound mirrored traffic from the monitor port can be sent out of the specified ethernet interface. If “None” appears instead of an ethernet interface number, it means that inbound mirrored traffic will not be sent out of this ethernet port.
Output	Indicates that outbound mirrored traffic from the monitor port can be sent out of the specified ethernet interface. If “None” appears instead of an ethernet interface number, it means that outbound mirrored traffic will not be sent out of this ethernet port.
Port monitored at ingress	Port(s) whose inbound traffic is copied to the monitor port.
Port monitored at egress	Port(s) whose outbound traffic is copied to the monitor port.

show monitor

Description Display the event thresholds for system resources.

Syntax

```
show monitor
```

Mode All

Example Below is an example output for this command:

```
ACOS#show monitor
Current system monitoring threshold:
Hard disk usage:     85
Memory usage:        95
Control CPU usage:   90
Data CPU usage:      90
IO Buffer usage:     2936012
Buffer Drop:         1000
Warning Temperature: 68
Conn type 0:         32767
Conn type 1:         32767
Conn type 2:         32767
Conn type 3:         32767
Conn type 4:         32767
SMP type 0:          32767
SMP type 1:          32767
SMP type 2:          32767
SMP type 3:          32767
SMP type 4:          32767
```

show netflow

Description Display NetFlow information.

Syntax

```
show netflow {common | monitor [monitor-name]}
```

Parameter	Description
common	Displays the currently configured maximum queue time for NetFlow export packets.

Parameter	Description
monitor [*monitor-name*]	Displays information for NetFlow monitors.

Mode All

Example The following example shows the configuration of a NetFlow monitor:

```
ACOS(config)#show netflow monitor
Netflow Monitor netflow-1
Protocol                          Netflow v10 (IPFIX)
   Status:                        Enable
   Filter:                        Global
   Destination:                   6.6.6.100:9996
   Source IP Use MGMT:            No
   Flow Timeout:                  10 Minutes
   Resend Template Per Records:   1
   Resend Template Timeout:       1800 Seconds
   Sent:                          110 (Pkts) / 11308 (Bytes)
   Records:                       Not Configured
   Custom-Records:
      sesn-event-nat44-creation     (Template: test2): 0
(records) / 0 (fails)
      sesn-event-nat44-deletion     (Template: test2): 0
(records) / 0 (fails)
      sesn-event-nat64-deletion     (Template: test2): 0
(records) / 0 (fails)
      sesn-event-nat64-creation     (Template: test2): 0
(records) / 0 (fails)
      sesn-event-dslite-creation    (Template: test2): 0
(records) / 0 (fails)
      sesn-event-dslite-deletion    (Template: test2): 0
(records) / 0 (fails)
      sesn-event-fw4-creation       (Template: test2): 0
(records) / 0 (fails)
      sesn-event-fw4-deletion       (Template: test2): 0
(records) / 0 (fails)
      sesn-event-fw6-creation       (Template: test2): 0
(records) / 0 (fails)
```

```
      sesn-event-fw6-deletion       (Template: test2): 0
(records) / 0 (fails)
      deny-reset-event-fw4          (Template: test2): 0
(records) / 0 (fails)
      deny-reset-event-fw6          (Template: test2): 0
(records) / 0 (fails)
      port-mapping-nat44-creation   (Template: test2 0
(records) / 0 (fails)
      port-mapping-nat44-deletion   (Template: test2): 0
(records) / 0 (fails)
      port-mapping-nat64-creation   (Template: test2): 0
(records) / 0 (fails)
      port-mapping-nat64-deletion   (Template: test2 0
(records) / 0 (fails)
      port-mapping-dslite-creation  (Template: test2) 0
(records) / 0 (fails)
      port-mapping-dslite-deletion  (Template: test2) 0
(records) / 0 (fails)
      port-batch-nat44-creation     (Template: test): 0
(records) / 0 (fails)
      port-batch-nat44-deletion     (Template: test): 0
(records) / 0 (fails)
      port-batch-nat64-creation     (Template: test): 0
(records) / 0 (fails)
      port-batch-nat64-deletion     (Template: test): 0
(records) / 0 (fails)
      port-batch-dslite-creation    (Template: test): 0
(records) / 0 (fails)
      port-batch-dslite-deletion    (Template: test): 0
(records) / 0 (fails)
      port-batch-v2-nat44-creation  (Template: test): 0
(records) / 0 (fails)
      port-batch-v2-nat44-deletion  (Template: test): 0
(records) / 0 (fails)
      port-batch-v2-nat64-creation  (Template: test): 0
(records) / 0 (fails)
      port-batch-v2-nat64-deletion  (Template: test): 0
(records) / 0 (fails)
```

```
      port-batch-v2-dslite-creation (Template: test): 0
(records) / 0 (fails)
      port-batch-v2-dslite-deletion (Template: test): 0
(records) / 0 (fails)
```

The following table shows the descriptions of the command output:

Field	Description
Protocol	Specifies the NetFlow Protocol version (NetFlow v9 or NetFlow v10/IPFIX)
Status	Specifies whether or not the NetFlow monitor is enabled.
Filter	Identifies the specific type and subset of resources that are being monitored (global, specific ports, or a NAT pool).
Destination	Indicates the destination IP address and port, if configured.
Source IP Use MGMT	Specifies whether the IP address of the management port of the ACOS Device is being used as the source IP of NetFlow packets.
Flow Timeout	Timeout value interval at which flow records are periodically exported for long-lived sessions. Flow records for short-lived sessions (if any) are sent upon termination of the session.
Resend Template Per Records	The number of records before the ACOS Device resends the NetFlow template that describes the data to perform a refresh of the template on the NetFlow collector.
Resend Template Timeout	The amount of time before the ACOS Device resends the template that describes the data to perform a refresh of the template on the NetFlow collector.
Sent	Total number of NetFlow packets and bytes sent.
Records	Specifies the NetFlow template types configured, which define the NetFlow records to export.

Field	Description
Custom Records	Specifies the NetFlow template custom record configured, which define the IPFIX records to export.

show ntp

Description Show the Network Time Protocol (NTP) servers and status.

Syntax

```
show ntp {servers | status}
```

Parameter	Description
servers	Lists the configured NTP servers and their state (enabled/disabled).
status	Lists the configured NTP servers and the status of the connection between ACOS and the server.

Mode Privileged EXEC level and configuration levels

Example The following commands show NTP information:

```
ACOS#show ntp servers
Ntp Server                        isPreferred Mode
Authentication
-------------------------------------------------------------------
--------------
 10.255.254.50                  no          enabled  disabled
 10.255.249.43                  no          enabled  disabled

ACOS#show ntp status
NTP Server                             Status
-----------------------------------------
10.255.254.50                  synchronized
10.255.249.43                       polling
```

show pbslb

Description Show configuration information and statistics for Policy-based SLB (PBSLB).

Syntax

```
show pbslb

show pbslb client [bandwidth | ip address]

show pbslb service-group [name]

show pbslb statistics

show pbslb system

show pbslb virtual-server [bandwidth | virtual-server name]
[port port-num | rsp-code-limit port{port-num} ]
```

Field	Description
client [*bandwidth*| *ip address*]	Shows PBSLB client statistics by rate-limiting bandwidth or IP address (IPv4 and IPv6).
service-group [name]	Shows PBSLB statistics of the specified service-group.
statistics	Shows PBSLB statistics information.
system	Shows PBSLB system-wide statistics.
virtual-server *[bandwidth | virtual-server name]* [**port** *port-num* | **rsp-code-limit port** *{port-num}*]	Shows PBSLB statistics of the rate-limiting bandwidth or specified virtual server. • **port** *port-num* – Shows statistics of the specified virtual port number. • **rsp-code-limit port** *{port-num}* - Shows PBSLB server response code limit of the virtual port.

Mode All

Example The following command shows PBSLB information for an ACOS Device:

```
ACOS#show pbslb
Virtual server class list statistics:
```

```
F = Flag (C-Connection, R-Request, S-Response code, D-direct
action), Over-L = Over-limit, Over-RL = Over rate limit, LkupT
= Lockup time left, Lkup# = Lockup number
when F=S; Rcode = response code range, Rate = number of RSP
code in period
when F=D; Please use the description with ()
Source  Destination  Rcode  F Current Rate Over-L  Over-RL
LkupT Lkup# Age
(lid num)                  (D)(drop) (Reset)(Ser-sel)(Ser-sel-
fail)  (Age)
---------------+-----------+-+--------+------+--------+-------
-+----+----+
1.1.1.91  1.1.1.120:80     C 0        0      0        0
0    0    5
Total: 1


Client class list statistics:
F = Flag (C-Connection, R-Request, S-Response code, D-direct
action), Over-L = Over-limit, Over-RL = Over rate limit, LkupT
= Lockup time left, Lkup# = Lockup number
when F=S; Rcode = response code range, Rate = number of RSP
code in period
when F=D; Please use the description with ()
Source  Destination  Rcode F  Current Rate Over-L  Over-RL
LkupT Lkup# Age
(lid num)                  (D) drop) (Reset)(Ser-sel)(Ser-sel-
fail)(Age)
---------------+-----------+-+------+------+---------+--------
-+-----+---+
1.1.1.91  1.1.1.120:80     C 0      0      0         0
0     0  5
Total: 1
```

The following table describes the fields in the command output.

Field	Description
Source	Indicates source address.

Field	Description
Destination	Indicates destination address.
Flag	Indicates whether the row of information applies to connections or requests: • C – The statistics listed in this row are for connections. • R – The statistics listed in this row are for HTTP requests. • S - The statistics listed in this row are for HTTP response code. • D - The statistics listed in this row are direct actions.
Current	Indicates current number of connections or requests.
Rate	Indicates current connection or request rate, which is the number of connections or requests per second.
Over-L (Over-limit)	Indicates number of times client connections or requests exceeded the configured limit.
Over-RL (Over rate limit)	Indicates number of times client connections or requests exceeded the configured rate limit.
LkupT (Lockup time left)	Indicates number of lockup time left before the ACOS device locks up the ICMP traffic on the interface.
Lkup# (Lockup number)	Indicates current lockup number.
Age	Indicates configured global PBSLB entry age or the default PBSLB entry age (6 minutes).

Example The following command shows information about client-side statistics related to PBSLB:

```
ACOS#show pbslb client
Client class list statistics:
F = Flag (C-Connection, R-Request, S-Response code, D-direct
action), Over-L = Over-limit, Over-RL = Over rate limit, LkupT
= Lockup time left, Lkup# = Lockup number
      when F=S; Rcode = response code range, Rate = number of
RSP code in period
                                    when F=D; Please use the
description with ()
Source          Destination           Rcode  F   Current
Rate       Over-L  Over-RL   LkupT Lkup# Age
(lid num)                                    (D)  (drop)
(Reset)  (Ser-sel)  (Ser-sel-fail)        (Age)
---------------+-------------------+-------+-+---------+-----
----+----------+----------+-----+-----+----
2000::10:214:6: [2000::10:214:6:100]         C 0         0
    0          3          0      0      6  <<- limit_stat of
2               :53
                                               per vport
2000::10:214:6: *                            C 0         0
    0          5          0      0      6  <<- limit_stat of
2
                                           global-dns-cache
2000::10:214:6: *                            C 0         0
    0          3          0      0      6
12
Total: 3
```

The '*' symbol in the **Destination** field in the above output indicates that the traffic is targeting the entire partition for load balancing rather than individual virtual ports within the partition.

Example The following command shows PBSLB statistics information:

```
ACOS#show pbslb statistics
```

```
PBSLB Globals Stats
Current PBSLB entry Count                    : 0
Current PBSLB stat  Count                    : 0
PBSLB IPv4 entry created                     : 0
PBSLB IPv4 entry freed                       : 0
PBSLB IPv6 entry created                     : 0
PBSLB IPv6 entry freed                       : 0
PBSLB domain entry created                   : 0
PBSLB domain entry freed                     : 0
PBSLB direct action entry created            : 0
PBSLB direct action entry freed              : 0
Current PBSLB target global count            : 0
Current PBSLB target vserver count           : 0
Current PBSLB target vport count             : 0
Current PBSLB target LOC count               : 0
Current PBSLB target rserver count           : 0
Current PBSLB target rport count             : 0
Current PBSLB target service-group count     : 0
Current PBSLB target global DNS cache count : 0
```

show pki

Description Shows information about the certificates on the ACOS Device.

Syntax

```
show pki
{ca-cert [cert-name [detail]| cert [cert-name [detail]] | crl
| scep-cert-cert [log [word]| status]|
cmp-cert {[log cert-name [follow | from-start | num-lines] |
[status]} |
acme-cert {[log cert-name [follow | from-start | num-lines] |
[status]}
csr [cert-name [detail]] |
[partition {shared | partition-name} | sort-by]
```

Option	Description
ca-cert ***cert-name***	Shows the CA certificate. *cert-name* - Specifies a name for the certificate, and you can name with a maximum of 255 characters.

Option	Description
cert *cert-name*	Shows information about the certificates on the ACOS Device. To display information for a specific certificate, use the *cert-name* option. To display additional details about the certificate, use the **detail** option.
crl	Shows information about the Certificate Revocation Lists (CRLs) that have been imported to the ACOS Device.

cmp-cert *[log | status]*	Shows information about CMP certificate.
	• *log* - Shows cmp-cert enrollment log and debug information. Use CMP certificate name.
	`ACOS (config)# show pki cmp-cert log testingcert`
	• *status* - Shows CMP enrollment status.
	`ACOS(config)#show pki cmp-cert status`

scep-cert *[log | status]*	Shows information about SCEP certificate. • *log* - Shows scep-cert enrollment log and debug information. Use SCEP certificate name. • *status* - Shows SCEP enrollment status. `ACOS (config)# show pki scep-cert log testingcert`

acme-cert *[log | status]*	Shows information about ACME certificate.
	• *log* - Shows acme-cert enrollment log and debug information. Use follow, from-start, and num-lines for more details.
	`ACOS(config)#show pki acme-cert log test-https follow`
	`ACOS(config)#show pki acme-cert log test-https from-start`
	`ACOS (config-acme cert:test-https)# show pki acme-cert log test-https num-lines 30`

Option	Description
	• *status* - Shows ACME enrollment status. `ACOS(config)#show pki acme-cert status`
csr ***csr-name***	Shows information about the certificate signing requests. To display information for a specific certificate signing request, use the *csr-name* option. To display additional details about the certificate signing request, use the **detail** option.
[**partition {shared | partition-name}| sort-by**]	Allows you to view the certificates of the shared partition: **NOTE:** `partition {shared | partition-name}` is only supported in L3V partition. • *shared* - A specific partition. • *partition-name* - You can display information from the shared partition or from a specific L3V partition. • *sort-by* - Sort by the certificate files.

Mode All

Example The following command shows SSL certificate information:

```
ACOS(config)#pki create certificate server
input key bits(1024,2048,4096) default 1024:1024
input Common Name, 1~64:server
input Division, 0~31:division
input Organization, 0~63:org
input Locality, 0~31:sj
input State or Province, 0~31:ca
input Country, 2 characters:us
input email address, 0~64:
input valid days, 30~3650, default 730:

ACOS(config)#show pki cert
Name: server  Type: certificate/key  Expiration: Sep 13
18:35:26 2016 GMT [Unexpired, Unbound]
```

```
ACOS(config)#show pki ca-cert
Name                Type                          Expiration
Status
-------------------------------------------------------------------
---------
default_ca_bundle  certificate  Jan 28 12:00:00 2028 GMT
[Unexpired, Bound]
```

show poap

Description Display the Power On Auto Provisioning (POAP) mode.

Syntax

```
show poap
```

Mode All

Example Example command and output:

```
ACOS(config)#show poap
Disabled
```

show process system

Description Display the status of system processes.

Syntax

```
show process system
```

Mode Privileged EXEC level and configuration levels

Usage For more information, see “System Overview” chapter of the *System Configuration and Administration Guide.*

Example The following command shows the status of system processes on an ACOS Device:

```
ACOS#show process system
a10mon is running
syslogd is running
a10logd is running
a10timer is running
a10Stat is running
```

```
a10hm is running
a10switch is running
a10rt is running
a10rip is running
a10ospf is running
a10snmpd is running
a10gmpd is running
a10wa is running
a10lb is running
```

show radius-server

Description Display statistics about a RADIUS server.

Syntax

```
show radius-server
```

Example The following text is a sample output for this command:

```
ACOS(config)#show radius-server
Radius server              : 10.0.0.0
contact start              : 5
contact failed             : 3
authentication success     : 1
authentication failed      : 1
authorization success      : 1

Radius server              : 10.0.0.1
contact start              : 0
contact failed             : 0
authentication success     : 0
authentication failed      : 0
authorization success      : 0

ACOS(config)#
```

Mode All

show reboot

Description Display scheduled system reboots.

Syntax `show reboot`

Mode All

Example The following command shows a scheduled reboot on the ACOS Device:

```
ACOS#show reboot
Reboot scheduled for 20:00:00 GMT Thu Nov 30 2017 (in 7 hours
and 28 minutes) by admin on 172.17.2.46
Reboot reason: Scheduled reboot
```

show resource-accounting

Description View resource usage statistics.

Resource accounting limits can be configured with the system resource-accounting template command.

Syntax

```
show resource-accounting
[
all-partitions |
global |
partition {partition-name | shared} |
resource-type
 {app-resources | network-resources | system-resources}
[summary] |
summary
]
```

Parameter	Description
all-partitions	Lists resource usage counters for all partitions.
global	Lists global resource usage counters.
partition {*partition-name* | **shared**}	Lists resource usage counters for the specified partition.
resource-type	Lists resource usage counters filtered by the selected resource type, System, Network, or Application.
summary	Lists resource usage counters displayed in the

Parameter	Description
	summary output format. you can filter by a specific resource name and a usage value for that resource. The Current usage value is displayed by default if no value is specified.

Mode All

Example The following example shows example output for this command:

```
ACOS# show resource-accounting resource-type system-resources
Partition Shared     Resource   Current   Min-Guaranteed
Max-allowed Utilization(%)
Max-exceeded  Threshold-exceeded    Average Peak

Static Mac             0          0         500           0

0                 0              0         0
Static Arp             0          0         128           0

0                 0              0         0
Static Neighbor        0          0         128           0

0                 0              0         0
V4 Static route        0          0         4000          0

0                 0              0         0
V6 Static route        0          0         4000          0

0                 0              0         0
Object Group Count     0          0         4000          0

0                 0              0         0
Object Group Clause C  0          0         1024000       0

0                 0              0         0
V4 ACL Lines Count     10         0         16000         0

0                 0              0         10
```

```
V6 ACL Lines Count     0           0           16000          0

0                  0               0           0
Real Servers           14          0           1024           1

0                  0               0           14
Real Ports             21          0           2048           1

0                  0               0           21
GSLB Sites             0           0           1000           0

0                  0               0           0
GSLB Device            0           0           2000           0

0                  0               0           0
GSLB Service IP        0           0           1024           0

0                  0               0           0
GSLB Service Port      0           0           2048           0

0                  0               0           0
GSLB Zone              1           0           10000          0

0                  0               0           1
GSLB Service           2           0           20000          0

0                  0               0           2
GSLB Policy            1           0           20000          0

0                  0               0           1
GSLB IP List           0           0           1000           0

0                  0               0           0
GSLB Template          0           0           2000           0

0                  0               0           0
GSLB Geo-location      78          0           10000000       0

0                  0               0           78
```

```
GSLB Service-Group     0           0           500           0

0                  0               0           0
Service Group          49          0           512           9

0                  0               0           49
Virtual Server         10          0           512           1

0                  0               0           10
Health Monitor         6           0           1023          0

0                  0               0           6
```

The following table describes the columns in this output.

Field	Description
Resource	Lists the configured resources.
Current	Shows that resource's current usage value.
Min-Guaranteed	Shows the minimum guaranteed value for that resource.
Max-allowed	Shows the maximum value allowed for that resource.
Utilization(%)	Shows the CPU percentage utilization for that resource.
Max-exceeded	Shows when a resource exceeded its maximum allowed value.
Threshold-exceeded	Indicates the number of times that resources exceeded its usage threshold.
Average	Shows the average value or percentage of the specific resource.
Peak	Shows the highest value or percentage of the specific resource.

The following example shows a sample **summary** output:

```
ACOS# show resource-accounting resource-type system-resources
summary
```

```
Current/Average/Peak
 Current/Average/Peak Utilization %

System Resource    L4 Session Count  Concurrent Sessions L4
CPS L7 CPS        NAT CPS             SSL CPS            FW CPS
  SSL Throughput  Bandwidth
Partition shared   0%/0%/0%           0/0/0       0/0/0     0/0/0
 0/0/0         0/0/0               0/0/0              0/0/0
0/0/0     0/0/0  0/0/0         0/0/0                0/0/0
   0/0/0       0/0/0     0/0/0  0/0/0
```

This page displays the resource usage in the current partition for network, application, and system resources. The resources are provided in the following format:

```
Current Value / Average Value / Peak Value, and
Current Percentage / Average Percentage / Peak Percentage
```

The percentage numbers represent the percentage out of the maximum allowable value on your ACOS Device; for example, if a maximum of 4096 real servers can be configured on your device and 2048 are currently configured, the current percentage would be 50%.

show resource-tracked

Description Display the policy-based failover template details.

Syntax

```
show resource-tracked
```

Mode All

Example The following command shows the event information for all the policy-based failover templates:

```
ACOS (config)#show resource-tracked
Resource Tracking Name: template_1
bgp 12.12.10.1 weight 100
gateway 10.10.10.1 weight 100
route 20.20.20.0 /24 weight 100

User-Idx 1 | User name 100 | Cost 200
```

```
User-Idx 4| User name 104 | Cost 200

Resource Tracking Name: template_1
interface ethernet 1 weight 40
trunk 1 weight 20
vlan 2 timeout 20 weight 30

User-Idx 2| User name 102 | Cost 90
User-Idx 3| User name 103 | Cost 90

Totally 2 event(s) tracked
```

The following command shows the event information for specific template:

```
Resource Tracking Name: template_1
 bgp 12.12.10.1 weight 100
 gateway 10.10.10.1 weight 100
 route 20.20.20.0 /24 weight 100

User-Idx 1 | User name 100 | Cost 200
User-Idx 4| User name 104 | Cost 200

Totally 1 event(s) tracked
```

show resource-tracked-by-user

Description Display the policy-based failover template details.

Syntax

```
show resource-tracked
```

Mode All

Example The following command shows the event information for a template based on user information:

```
ACOS (config)#show resource-tracked

User-Idx 1 | User name 100 | Cost 200
 Resource Tracking Name: template_1
```

```
   bgp 12.12.10.1 weight 100
   gateway 10.10.10.1 weight 100
   route 20.20.20.0 /24 weight 100

User-Idx 4| User name 104 | Cost 200
 Resource Tracking Name: template_1
   bgp 12.12.10.1 weight 100
   gateway 10.10.10.1 weight 100
   route 20.20.20.0 /24 weight 100

User-Idx 2| User name 102 | Cost 90
 Resource Tracking Name: template_2
   interface ethernet 1 weight 40
   trunk 1 weight 20
   vlan 2 timeout 20 weight 30

User-Idx 3| User name 103 | Cost 90
 Resource Tracking Name: template_2
   interface ethernet 1 weight 40
   trunk 1 weight 20
   vlan 2 timeout 20 weight 30

Totally 4 event(s) tracked
```

show route-map

Description Show the configured route maps.

Syntax

```
show route-map [map-name]
```

Mode All

show router log file

Description Show router logs.

Syntax

```
show router log file
[
file-num |
bgpd [file-num] |
isisd [file-num] |
```

```
nsm [file-num] |
ospf6d [file-num] |
ospfd [file-num] |
ripd [file-num] |
ripngd [file-num]
]
```

Parameter	Description
file-num	Log file number.
bgpd [*file-num*]	Displays the specified BGP log file, or all BGP log files.
isisd [*file-num*]	Displays the specified IS-IS log file, or all IS-IS log files.
nsm [*file-num*]	Displays the specified Network Services Module (NSM) log file, or all NSM log files.
ospf6d [*file-num*]	Displays the specified IPv6 OSPFv3 log file, or all OSPFv3 log files.
ospfd [*file-num*]	Displays the specified IPv4 OSPFv2 log file, or all OSPFv2 log files.
ripd [*file-num*]	Displays the specified IPv4 RIP log file, or all IPv4 RIP log files.
ripngd [*file-num*]	Displays the specified IPv6 RIP log file, or all IPv6 RIP log files.

Mode All

show rpz

Description Display the configured Response Policy Zone (RPZ) files and the contents of a specified file.

Syntax

```
show rpz [filename]
```

Parameter	Description
filename	Specify the RPZ file name (1-64 characters).

Mode All

Example The following example displays the list of RPZ file(s) currently on the system and indicates whether each file is associated with a DNS template:

```
ACOS(config)# show rpz
Max RPZ file size: 61137K
Name                                                    DNS template
------------------------------------------------------------------------
rpztest                                                 No
test15M                                                 No
test16k                                                 No
test500k                                                No
Total RPZ number: 4
```

Example The following example displays the contents of the specified RPZ file:

```
ACOS (config)# show rpz A10.rpz
Name:               A10.rpz
Syntax:             Check
DNS template:       Bind
Content:
;
; BIND data file for local loopback interface
;
$TTL 1H
$ORIGIN rpz.
@   IN  SOA localhost. nobody.localhost (
2015103102
1h
15m
30d
2h )
NS localhost.
; DROP action
32.184.101.20.20.rpz-client-ip        IN CNAME rpz-drop.
  ; Client ip
32.2.0.185.23.rpz-ip                                    IN CNAME
rpz-drop.         ; Response IP
www.a10networks.com                                      IN
CNAME rpz-drop.         ; QNAME
```

```
ns-130.awsdns-16.com.rpz-nsdname           IN CNAME rpz-drop.
      ; NSDNAME
32.229.199.251.205.rpz-nsip                   IN CNAME rpz-
drop.          ; NSIP

; TCP-Only action
*.apple.com                              IN CNAME rpz-tcp-only.

; NXDOMAIN action
www.netflix.com                                          IN
CNAME .

; NODATA action
www.facebook.com                         IN CNAME *.

; IPv6 example
128.5.C0A8.FFFF.0.1.0.db8.2001.rpz-ip                        IN
CNAME rpz-drop.
64.5.ZZ.1.0.db8.800.rpz-ip                                   IN
CNAME rpz-drop.
```

show run

Description Displays the system level running-config.

This command is used to view the running-config in the partition where the command is issued. To view the running-config for a different partition, use the **show partition-config** command.

Syntax

```
show run[options]
```

Usage This command displays the entire running-config in the current partition.

To narrow the output to specific feature modules, use **show run ?** to view the available modules, then specify them from the command line. For example, to view the running-config related only to SLB servers, use:

Example The following example shows the running-config:

```
ACOS# show run
!Current configuration: 1174 bytes
!Configuration last updated at 09:08:43 IST Wed Aug 18 2021
!Configuration last saved at 08:58:03 IST Wed Aug 18 2021
!64-bit Advanced Core OS (ACOS) version 5.3.0 (Jun-28-
2021,13:28)
!offload-cpus 1
!
multi-config enable
!
terminal idle-timeout 0
!
class-list test_cl ac
contains mycompany
ends-with com
equals dev.mycompany.com
starts-with dev
!
vlan 11
tagged ethernet 1
router-interface ve 11
!
partition a10l3v1 id 1
!
hostname InsideAX
```

Example The following example shows the encrypted shared secret of the TACACS server configured for authentication:

```
ACOS(config)# show run
Current configuration: 384 bytes
!
multi-config enable
!
!
!
tacacs-server host 192.000 secret encrypted
fftthMgh/ruk5RlnvqT3rRI92/mrt9yjR4lk0Phz
!
interface management
  ip address 10.23.21.76 255.255.254.0
```

```
  ip default-gateway 10.23.20.1
!
!
!
```

show run visibility

Description Display network statistics or visibility.

Syntax

```
show run visibility
```

Default NA

Mode Normal mode

Example

```
ACOS(config)# show run visibility
!Section configuration: 130 bytes
!
visibility
  topk source-entity
  reporting
    sampling-enable all
    template notification name
  monitor traffic dest
!
ACOS(config)# show run visibility anomaly-detection
!Section configuration: 0 bytes
ACOS(config)# show run visibility reporting
!Section configuration: 49 bytes
sampling-enable all
template notification name
!
```

show running-config

Description Displays the running-config.

This command is used to view the running-config in the partition where the command is issued. To view the running-config for a different partition, use the **show partition-config** command.

Syntax

```
show running-config [options]
```

Usage

This command displays the entire running-config in the current partition.

To narrow the output to specific feature modules, use **show running-config ?** to view the available modules, then specify them from the command line. For example, to view the running-config related only to SLB servers, use:

```
show running-config slb server
```

Example

The following example shows the running-config for SLB virtual servers:

```
ACOS(config)# show running-config slb virtual-server
!Section configuration: 2 bytes
!
slb virtual-server test-vip 10.10.10.15
  port 80 tcp
!
!
end
ACOS(NOLICENSE)#
```

Example

This example shows how to use the **aflex-scripts** options to view configured aFleX scripts:

```
ACOS(config)# show running-config all-partitions aflex-scripts
!Current configuration: 1044 bytes
!Configuration last updated at 17:36:35 IST Wed Jun 14 2016
!Configuration last saved at 17:35:40 IST Wed Jun 14 2016
!version 4.1.1, build 25 (Jun-14-2016,08:26)
!...
Name:                    logging_clients
Syntax:                  Check
Virtual port:            No
# This aFleX logs Client/Server IP/Port information for
security when using Source NAT when CLIENT_ACCEPTED {
```

```
  set timestamp [TIME::clock seconds]
  set cip [IP::client_addr]
  set cport [TCP::client_port]
  set vip [IP::local_addr]
  set vport [TCP::local_port]
}
when SERVER_CONNECTED {
  set sip [IP::server_addr]
  set sport [TCP::server_port]
  set snat_ip [IP::local_addr]
  set snat_port [TCP::local_port]
  log "\[$timestamp\] $cip:$cport -> $vip:$vport to $snat_
ip:$snat_port -> $sip:$sport"
}
--MORE--
```

Example This example shows the sequence number of the rule in the access-list:

```
ACOS(config)# show running-config
!Current configuration: 690 bytes
!Configuration last updated at 06:14:14 IST Wed Oct 5 2022
!Configuration last saved at 06:52:47 IST Wed Oct 5 2022
!64-bit Advanced Core OS (ACOS) version 6.0.0-d, build 326
(Sept-21-2022,23:08)
!
!
access-list 60 4 deny 5.1.1.1 0.0.0.0
!
access-list 60 20 deny 5.1.1.2 0.0.0.0
!
access-list 160 4 deny ip 6.1.1.1 0.0.0.0 any
!
access-list 160 40 deny ip 6.1.1.2 0.0.0.0 any
!
ip access-list acl_sample_ipv4
  4 deny ip 7.1.1.1 0.0.0.0 any
  55 deny ip 7.1.1.2 0.0.0.0 any
!
ipv6 access-list acl_sample_ipv6
  4 deny ipv6 68::55:6:78/128 any
  50 deny ipv6 68::55:6:79/128 any
```

```
!
```

Example The following example shows the running-config for SLB resource usage:

```
ACOS(config)# show running-config slb resource-usage | inc slb
resource-usage pbslb-entry-count
slb resource-usage pbslb-entry-count 32000000
```

Example The following example shows the encrypted shared secret of the TACACS server configured for authentication:

```
ACOS(config)# show running config
Current configuration: 384 bytes
!
multi-config enable
!
!
!
tacacs-server host 192.000 secret encrypted
fftthMgh/ruk5RlnvqT3rRI92/mrt9yjR4lk0Phz
!
interface management
  ip address 10.23.21.76 255.255.254.0
  ip default-gateway 10.23.20.1
!
!
!
```

show session

Description Display session information.

Syntax

```
show session
[
brief |
blacklist-sessions |
diameter [session-id string] |
dns-id-switch |
ds-lite [suboptions]|
filter {name | config} |
full-width
http2
ipv4 [addr-suboptions] |
ipv6 [addr-suboptions] |
nat44 [suboptions] |
```

```
nat64 [suboptions] |
persist [persistence-type[addr-suboptions]] |
radius |
sctp |
server [name] |
sip [addr-suboptions] |
sixrd-nat64 [suboptions] |
virtual-server [name]
]
```

Parameter	Description
brief	Displays summary statistics for all session types.
blacklist-sessions	Displays statistics for blacklist sessions.
diameter	Displays Diameter session information such as Session-Id, Forward Source, Forward Dest, Reverse Source, Reverse Dest, Hash, and Age. The following option is available: session-id *string* - Filter diameter sessions by string.
dns-id-switch	Displays statistics for DNS switch sessions.
ds-lite	Displays statistics for DS-Lite sessions. The following options are available: • **dest-port** *num*—View sessions with the specified destination port (1-65535). • **dest-v4-addr***ipaddr*[**/***length*]—View sessions with the specified destination IPv4 address. • **dest-v6-addr***ipaddr*[**/***length*]—View sessions with the specified destination IPv6 address. • **source-port** *num*—View sessions with the specified source port (1-65535). • **source-v4-addr***ipaddr*[**/***length*]—View sessions with the specified source IPv4 address. • **source-v6-addr***ipaddr*[**/***length*]—View sessions with the specified source IPv6 address. Not all suboptions are available for use in

Parameter	Description
	conjunction with others. For example, if the first suboption you enter is **dest-v4-addr**, the only additional suboption you can specify is **dest-port**.
filter {*name* | **config**}	Displays information about configured session filters. Specify **config** to view all configured session filters, or specify a filter *name* to view the specified filter only.
full-width	Display full IPv6 addresses. By default, IPv6 addresses are truncated to 22 characters.
http2	Displays HTTP2 information. Does not include information that is available through show http commands.
ipv4	Displays information for IPv4 sessions. The following address suboptions are available: • **dest-port** *num*—View sessions with the specified destination port (1-65535). • **dest-v4-addr***ipaddr*[**/***length*]—View sessions with the specified destination IPv4 address. • **source-port** *num*—View sessions with the specified source port (1-65535). • **source-v4-addr***ipaddr*[**/***length*]—View sessions with the specified source IPv4 address. Not all suboptions are available for use in conjunction with others. For example, if the first suboption you enter is **dest-v4-addr**, the only additional suboption you can specify is **dest-port**.
ipv6	Displays information for IPv6 sessions. The following address suboptions are available: • **dest-port** *num*—View sessions with the specified destination port (1-65535).

Parameter	Description
	• **dest-v6-addr***ipaddr*[**/***length*]—View sessions with the specified destination IPv6 address. • **source-port** *num*—View sessions with the specified source port (1-65535). • **source-v6-addr***ipaddr*[**/***length*]—View sessions with the specified source IPv6 address. Not all suboptions are available for use in conjunction with others. For example, if the first suboption you enter is **dest-v4-addr**, the only additional suboption you can specify is **dest-port**.
nat44	Displays information for NAT44 sessions. The supported suboptions are same as for **ipv4**.
nat64	Displays information for NAT64 sessions. The supported suboptions are same as for **ipv6**.
persist [*type* [*suboptions*]]	Displays session persistence information. The following persistence types can be specified: • **dst-ip**—Displays destination-IP persistent sessions. • ipv6—Displays IPv6 sessions. • **src-ip**—Displays source-IP persistent sessions. • **ssl-sid**—Displays SSL-session-ID persistent sessions. • **uie**—Displays sessions that are made persistent by the aFleX `persistuie` command. The available *suboptions* are the same as the ones for **ipv4**.

Parameter	Description
	NOTE: To clear persistent sessions, use the **clear sessions persist** command.
quic	Displays QUIC session information.
radius	Displays RADIUS session information.
sctp	Displays SCTP sessions only.
server [*name*]	Displays sessions for real servers, or a specific server *name*.
sip	Displays information for Session Initiation Protocol (SIP) sessions. The following suboptions are available: • **dest-port** *num*—View sessions with the specified destination port (1-65535). • **dest-v4-addr***ipaddr*[**/***length*]—View sessions with the specified destination IPv4 address. • **dest-v6-addr***ipaddr*[**/***length*]—View sessions with the specified destination IPv6 address. • **smp-sip-rtp** *num*—View SIP sessions.
sixrd-nat64	Displays 6rd-NAT64 session statistics. The available suboptions are the same as for **ds-lite**.
virtual-server [*name*]	Displays sessions for virtual servers, or a specific virtual server *name*.

Mode All

Usage For convenience, you can save session display options as a session filter.

NOTE: After entering the **clear session** command, the ACOS Device may remain in session-clear mode for up to 10 seconds. During this time, any new connections are sent to the delete queue for clearing.

Example The following command lists information for all IPv4 sessions:

```
ACOS(config)#show session ipv4
```

```
Traffic Type                          Total
----------------------------------------
Total Sessions                        1
TCP Established                       2
TCP Half Open                         0
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               0
Other                                 0
Reverse NAT TCP                       0
Reverse NAT UDP                       0
Free Buff Count                       0
Curr Free Conn                        2007033
Conn Count                            10
Conn Freed                            8
TCP SYN Half Open                     0
Blacklist sessions                    0
Blacklist sessions Created            13
Blacklist sessions Freed              13
Conn SMP Alloc                        13
Conn SMP Free                         2
Conn SMP Aged                         2
Conn Type 0 Available                 3997696
Conn Type 1 Available                 2031615
Conn Type 2 Available                 999424
Conn Type 3 Available                 499712
Conn Type 4 Available                 249856
Conn SMP Type 0 Available             3997696
Conn SMP Type 1 Available             1998848
Conn SMP Type 2 Available             999424
Conn SMP Type 3 Available             507875
Conn SMP Type 4 Available             249856
Total Local Sessions                  0
Prot Forward Source          Forward Dest    Reverse Source
    Reverse Dest           Age   Hash Flags Type
-------------------------------------------------------------
---------------------------------------------
Tcp  1.0.4.147:49107         1.0.100.1:21
1.0.3.148:21           1.0.4.147:49107        120   2 OS
```

```
Tcp  1.0.16.2:58736          1.0.100.1:21
1.0.3.148:21            1.0.16.2:58736          60     2 OS
Total Sessions:           2
```

The following table describes the fields in the command output.

Field	Description
TCP Established	Number of established TCP sessions.
TCP Half Open	Number of half-open TCP sessions. A half-open session is one for which the ACOS Device has not yet received a SYN ACK from the backend server.
SCTP Established	Number of established SCTP sessions.
SCTP Half Open	Number of half-open SCTP sessions. A half-open session is one for which the ACOS Device has not yet received a SYN ACK from the backend server.
UDP	Number of UDP sessions.
Non TCP/UDP IP sessions	Number of IP sessions other than TCP or UDP sessions. This counter applies specifically to IP protocol load balancing. For more information, see “IP Protocol Load Balancing” chapter in the *Application Delivery and Server Load Balancing Guide*.)
Other	Number of internally used sessions. As an example, internal sessions are used to hold fragmentation information.
Reverse NAT TCP	Number of reverse-NAT TCP sessions.
Reverse NAT UDP	Number of reverse-NAT UDP sessions.
Free Buff Count	Number of IO buffers currently available.
Curr Free	Number of Layer 4 sessions currently available.

Field	Description
Conn	
Conn Count	Number of connections.
Conn Freed	Number of connections freed after use.
TCP SYN Half Open	Number of half-open TCP sessions. These are sessions that are half-open from the client's perspective.
Blacklist sessions	Number of blacklist sessions currently active.
Blacklist sessions Created	Number of blacklist sessions created.
Blacklist sessions Freed	Number of blacklist sessions freed.
Conn SMP Alloc	Statistics for session memory resources.
Conn SMP Free	
Conn SMP Aged	
Conn Type 0-4 Available	
Conn SMP Type 0-4 Available	
Prot	Transport protocol.
Forward Source	Client IP address when connecting to a VIP. Notes: • For DNS sessions, the client's DNS transaction ID is shown instead of a protocol port number. • The output for connection-reuse sessions shows

Field	Description
	0.0.0.0 for the forward source and forward destination addresses. • For source-IP persistent sessions, if the option to include the client source port (`incl-sport`) is enabled in the persistence template, the client address shown in the Forward Source column includes the port number. • IPv4 client addresses – The first two bytes of the displayed value are the third and fourth octets of the client IP address. The last two bytes of the displayed value represent the client source port. For example, "155.1.1.151:33067" is shown as "1.151.129.43". • IPv6 client addresses – The first two bytes in the displayed value are a "binary OR" of the first two bytes of the client's IPv6 address and the client's source port number. For example, "2001:ff0:2082:1:1:1:d1:f000" with source port 38287 is shown as "b58f:ff0:2082:1:1:1:d1:f000".
Forward Dest	VIP to which the client is connected.
Reverse Source	Real server's IP address. **NOTE:** If the ACOS Device is functioning as a cache server (RAM caching), asterisks (*) in this field and the Reverse Dest field indicate that the ACOS Device directly served the requested content to the client from the ACOS RAM cache. In this case, the session is actually between the client and the ACOS Device rather than the real server.
Reverse Dest	IP address to which the real server responds.

Field	Description
	• If source NAT is used for the virtual port, this address is the source NAT address used by the ACOS Device when connecting to the real server. • If source IP NAT *is not* used for the virtual port, this address is the client IP address.
Age	Number of seconds before the session times out (increments of 60 seconds)
Hash	CPU ID.
Flags	These are internal flags used for debugging purposes by A10 Technical Support. They identify various attributes of a session such as traffic processing path (Fast or Slow), session forwarding (Software or Hardware) and more.
Type	Indicates the session type, which can be one of the following: • SLB-L4 – SLB session for Layer 4 traffic. • SLB-L7 – SLB session for Layer 7 traffic. • LSN - LSN session • NAT – Network Address Translation (NAT) session for dynamic NAT. • ST-NAT – NAT session for static NAT. • FIXED-NAT - Fixed NAT session. • ACL – Session for an ACL. • TCS – Transparent Cache Switching session. • XNT – Transparent session. • FIREWALL - Firewall session. • FW-BLACKLIST - Firewall Blacklist session.

The following counters apply only to the current partition:

- TCP Established
- TCP Half Open

- UDP
- Non TCP/UDP IP sessions
- Other
- Reverse NAT TCP
- Reverse NAT UDP

The other counters apply to all partitions, regardless of the partition from which the command is entered.

Example The following command displays the IPv4 session for a specific source IP address:

```
ACOS(config)#show session ipv4 source-v4-addr 1.0.4.147
Prot Forward Source          Forward Dest           Reverse
Source          Reverse Dest           Age    Hash Flags
-----------------------------------------------------------
-------------------------------------------
Tcp  1.0.4.147:49107         1.0.100.1:21
1.0.3.148:21           1.0.4.147:49107         120    2 OS
Total Sessions:           1
```

Example The following commands display IPv4 source-IP persistent sessions, clear one of the sessions, then verify that the session has been cleared:

```
ACOS(config)#show session persist src-ip
Prot Forward Source    Forward Dest           Reverse Source
     Age    Hash Flags
-----------------------------------------------------------
----------------------
src  1.0.16.2          1.0.100.1:21           1.0.3.148
6000  120    2    OS
src  1.0.4.147         1.0.100.1:21           1.0.3.148
6000  120    2    OS
Total Sessions:           2
ACOS(config)#clear sessions persist src-ip source-addr
1.0.16.2
ACOS(config)#show session persist src-ip
Prot Forward Source    Forward Dest           Reverse Source
     Age    Hash Flags
```

```
------------------------------------------------------------------
----------------------
src  1.0.4.147        1.0.100.1:21           1.0.3.148
 5880  2    OS
```

In this example, IPv4 source-IP persistent sessions are shown. The incl-sport option in the source-IP persistence template is enabled, so the value shown in the Forward Source column is a combination of the client source IP address and source port number. The first two bytes of the displayed value are the third and fourth octets of the client IP address. The last two bytes of the displayed value represent the client source port.

Example The following commands display IPv6 source-IP persistent sessions:

```
ACOS(config)#show session persist ipv6
Prot Forward Source
     Forward Dest
     Reverse Source
Age
------------------------------------------------------------------
----
src  [2001:ff0:2082:1:1:1:d1:f000]
     [2001:ff0:2082:1:1:1:f000:1111]:80
     [2001:ff0:2082:4:1:1:f000:1e4]:6880
300
```

In the output above, the Forward Source column shows the client's IPv6 address but does not show the port number. The port number is omitted because the **incl-sport** option in the source-IP persistence template is disabled.

In the output below, the same client IPv6 address is shown. However, in this case, the **incl-sport** option in the source-IP persistence template is enabled. Therefore, the Forward Source column includes the port number. The first two bytes in the displayed value are a "binary OR" of the first two bytes of the client's IPv6 address and the client's source port number. In this example, the Forward source value is "b58f:ff0:2082:1:1:1:d1:f000". The first two bytes, "b58f", are a "binary OR" value of "2001" and port number 38287.

```
ACOS(config)#show session persist ipv6
```

```
Prot Forward Source
     Forward Dest
     Reverse Source
Age
-----------------------------------------------------------------
----
src  [b58f:ff0:2082:1:1:1:d1:f000]
     [2001:ff0:2082:1:1:1:f000:1111]:80
     [2001:ff0:2082:4:1:1:f000:1e3]:6880
300
```

Example The following command shows active RADIUS sessions:

```
ACOS#show session radius
Traffic Type                          Total
-----------------------------------------
TCP Established                       0
TCP Half Open                         0
UDP                                   30
...

Prot Forward Source          Forward Dest           Reverse
Source         Reverse Dest           Age   Hash Flags Radius
ID
-----------------------------------------------------------------
---------------------------
Udp   10.11.11.50:32836      10.11.11.90:1812
10.11.11.15:1812       10.11.11.50:32836      120   1    NSe0
104
Udp   10.11.11.50:32836      10.11.11.90:1812
10.11.11.12:1812       10.11.11.50:32836      120   1    NSe0
111
...
Udp   10.11.11.50:32836      10.11.11.90:1812
10.11.11.14:1812       10.11.11.50:32836      120   7    NSe0
103
Udp   10.11.11.50:32836      10.11.11.90:1812
10.11.11.11:1812       10.11.11.50:32836      120   7    NSe0
222
Total Sessions:          30
```

The session table contains a separate session for each RADIUS Identifier value. The following address information is shown for each session:

- Forward Source – The sender of the RADIUS message. This is the IP address of the BRAS.
- Forward Dest – The RADIUS VIP on the ACOS Device.
- Reverse Source – The RADIUS server to which the ACOS Device sends requests that have the Identifier listed in the RADIUS ID field.
- Reverse Dest – The destination of the RADIUS server reply forwarded by the ACOS Device. (This is the sender of the initial RADIUS message that started the session, the BRAS in the example above.)

Example

The following example displays the output when viewing the sessions on a real server named “s2” whose IP address is 172.16.1.11:

```
ACOS(config)#show session server s2
Traffic Type Total
-----------------------------------------
TCP Established                          5
TCP Half Open                            0
UDP                                      0
Non TCP/UDP IP sessions                  0
Other                                    0
Reverse NAT TCP 0
Reverse NAT UDP                          0
Curr Free Conn                           2018015
Conn Count                               47300
Conn Freed                               46529
TCP SYN Half Open                        0
Conn SMP Alloc                           22
Conn SMP Free                            0
Conn SMP Aged                            0
Conn Type 0 Available                    3866493
Conn Type 1 Available                    1932797
Conn Type 2 Available                    950272
Conn Type 3 Available                    482942
Conn Type 4 Available                    241406
Conn SMP Type 0 Available                3801088
```

```
Conn SMP Type 1 Available                1900544
Conn SMP Type 2 Available                950272
Conn SMP Type 3 Available                483305
Conn SMP Type 4 Available                237568
Prot Forward Source Forward Dest Reverse Source Reverse
DestAge Hash Flags Type
-----------------------------------------------------------------
----------------
Tcp 172.16.2.10:59992 172.16.2.200:80 172.16.1.11:80
172.16.1.50:18254
600 1 NSe1 SLB-L7
Tcp 172.16.2.10:60171 172.16.2.200:44333 172.16.1.11:80
172.16.1.50:18253
600 1 NSe1 SLB-L7
Total Sessions: 2
```

Example The following command lists information for all Diameter sessions.

```
ACOS(config)#show session diameter
Traffic Type                          Total
-------------------------------------------
Diameter Entry Count                  4
Diameter Entry Freed                  0
Concurrent user-session               4

Session-Id
Forward Source    Forward Dest      Reverse Source    Reverse
Dest      Hash  Age
-----------------------------------------------------------------
-------------------------
client123.cswu.com;1464201606;3;app_test
10.1.1.33:7039    10.1.1.90:3868    10.2.2.32:3868
10.2.2.98:2104    5:5   600(600)
client123.cswu.com;1464201606;2;app_test
10.1.1.33:7039    10.1.1.90:3868    10.2.2.32:3868
10.2.2.98:2104    5:5   600(600)
client123.cswu.com;1464201606;1;app_test
10.1.1.33:7039    10.1.1.90:3868    10.2.2.30:3868
10.2.2.98:2084    5:5   600(600)
client123.cswu.com;1464201606;5;app_test
```

```
10.1.1.33:7039    10.1.1.90:3868    10.2.2.32:3868
10.2.2.98:2104    5:5    600(600)
```

Table 13 describes the new fields in the command output.

Table 13 : show session diameter fields

Field	Description
Session-Id	The unique ID that identifies the Diameter session.
Forward Source	The forward source client-ip:port.
Forward Dest	The forward destination vip-ip:port.
Reverse Source	The reverse source server-ip:port.
Reverse Dest	The reverse destination snat-ip:port.
Hash	The client-cpu:server-cpu hash.
Age	The current-timeout (session-age).

Example The following command lists brief information for all Diameter sessions:

```
ACOS(config)#show session diameter brief
Traffic Type                          Total
-------------------------------------------
Diameter Entry Count                  51122115
Diameter Entry Freed                  35212877
Concurrent user-session               15909238
```

Table 14 describes the new fields in the command output.

Table 14 : show session diameter brief fields

Field	Description
Diameter Entry Count	Total Diameter sessions created.
Diameter Entry Freed	Total Diameter sessions freed.
Concurrent user-session	Current simultaneous Diameter sessions.

Example The following command displays the statistics for blacklist sessions:

```
ACOS(config)# show session blacklist-sessions
```

```
Traffic Type                          Total
--------------------------------------------
Total Sessions                        1
TCP Established                       0
TCP Half Open                         0
Server TCP Established                0
Server TCP Half Open                  0
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               1
Other                                 0
Reverse NAT TCP                       0
Reverse NAT UDP                       0
Curr Free Conn                        2039791
Conn Count                            2
Conn Freed                            1
TCP SYN Half Open                     0
Blacklist sessions                    1
Blacklist sessions Created            2
Blacklist sessions Freed              1
Conn SMP Alloc                        7
Conn SMP Free                         0
Conn SMP Aged                         0
Conn Type 0 Available                 3670016
Conn Type 1 Available                 1998843
Conn Type 2 Available                 933886
Conn Type 3 Available                 458752
Conn Type 4 Available                 229376
Conn SMP Type 0 Available             3670016
Conn SMP Type 1 Available             1835008
Conn SMP Type 2 Available             917504
Conn SMP Type 3 Available             466936
Conn SMP Type 4 Available             229376
Total Local Sessions                  0
Prot Forward Source            Forward Dest               Reverse Source
        Reverse Dest              Age   Hash Flags              Type
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
```

```
Udp  172.16.25.204:1024         172.16.35.205:1024         0.0.0.0
        0.0.0.0                      2      4     NFe0f0r0          FW-BLACKLIST
Total Sessions:  1
```

The field descriptions are the same as those in Field. Additionally, the **Type** field indicates that the session is a blacklist session.

Related Commands:

- session-filter

show sflow

Description Show sFlow information.

Syntax

```
show sflow statistics
```

Mode All

show shutdown

Description Display scheduled system shutdowns.

Syntax

```
show shutdown
```

Mode Privileged EXEC level and configuration levels

Example The following command shows a scheduled shutdown on an ACOS Device:

```
ACOS# show shutdown
Shutdown scheduled for 14:50:00 GMT Thu Nov 30 2017 (in 2
hours and 40 minutes) by admin on 172.17.2.46
Shutdown reason: Scheduled shutdown
ACOS#.
```

show smtp

Description Display SMTP information.

Syntax

```
show smtp
```

Mode All

Example The following command shows the SMTP server address:

```
ACOS#show smtp
SMTP server address:          192.168.1.99
```

show snmp engineID

Description Displays the SNMPv3 engineID with its VCS status.

Prerequisite The snmp service should be enabled and SNMPv3 engineID should be set for the ACOS Device.

Syntax

```
show snmp engineID
```

Mode Global configuration

Example The following example shows the output of **show snmp engineID** command:

```
ACOS#show snmp engineID
EngineID: 80001f8804393837363534333231 30 VCS-LOCAL-ONLY
```

Related Commands:

- snmp-server enable service
- snmp-server engineID

show snmp oid

Description Displays SNMP OIDs.

For more information, see *MIB Reference*.

Syntax

```
show snmp oid
{
  server [svr-name] [port portnum] |
  service-group [sg-name] [addr-type {firewall | tcp | udp}]
    [port portnum] [server-member name] |
  virtual-server [vs-name] [port portnum]}
```

Parameter	Description
server *svr-name*	Returns OIDs for the axServerStatTable. If a *name* is specified, this command returns OIDs for the axServerPortStatTable.
service-group *sg-name*	Returns OIDs for the axServiceGroupStatTable. If a *name* is specified, this command returns OIDs for the axServerPortStatTable. You can narrow the command output by specifying the IP address type for **addr-type** or specific service-group *member*. Valid address types are **firewall**, **tcp**, or **udp**.
virtual-server *vs-name*	Returns OIDs for the axVirtualServerStatTable. If a *name* is specified, this command returns OIDs for the axVirtualServerPortStatTable.
port *port-num*	Returns OIDs for the specific port of a virtual server. If no port is specified, this command returns OIDs for all virtual port entries of the specified VIP.

Mode All

Example The sample command output below narrows the displayed OIDs for TCP IP addresses:

```
ACOS#show snmp oid service-group sg1 addr-type tcp
OID for axServiceGroupMemberStatTable
service-group-name sg1: type 2: server-name s2: port 80
============================================================
============
    axServiceGroupMemberStatName:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.1.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatAddrType:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.2.3.115.103.49.2.2.115.50.80
    axServerNameInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.3.3.115.103.49.2.2.115.50.80
```

```
    axServerPortNumInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.4.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatPktsIn:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.5.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatBytesIn:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.6.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatPktsOut:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.7.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatBytesOut:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.8.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatPersistConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.9.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatTotConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.10.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatCurConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.11.3.115.103.49.2.2.115.50.80
    axServerPortStatusInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.12.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatTotalL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.13.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatTotalCurrL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.14.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatTotalSuccL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.15.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatResponseTime:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.16.3.115.103.49.2.2.115.50.80
    axServiceGroupMemberStatPeakConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.17.3.115.103.49.2.2.115.50.80
service-group-name sg1: type 2: server-name s1: port 80
============================================================
============
    axServiceGroupMemberStatName:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.1.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatAddrType:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.2.3.115.103.49.2.2.115.49.80
    axServerNameInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.3.3.115.103.49.2.2.115.49.80
    axServerPortNumInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.4.3.115.103.49.2.2.115.49.80
```

```
    axServiceGroupMemberStatPktsIn:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.5.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatBytesIn:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.6.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPktsOut:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.7.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatBytesOut:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.8.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPersistConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.9.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.10.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatCurConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.11.3.115.103.49.2.2.115.49.80
    axServerPortStatusInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.12.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotalL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.13.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotalCurrL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.14.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotalSuccL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.15.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatResponseTime:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.16.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPeakConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.17.3.115.103.49.2.2.115.49.80
```

Example This output narrows the displayed OIDs for the service-group member “s1”:

```
ACOS#show snmp oid service-group sg1 server-member s1
OID for axServiceGroupMemberStatTable
service-group-name sg1: type 2: server-name s1: port 80
============================================================
============
    axServiceGroupMemberStatName:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.1.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatAddrType:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.2.3.115.103.49.2.2.115.49.80
```

```
    axServerNameInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.3.3.115.103.49.2.2.115.49.80
    axServerPortNumInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.4.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPktsIn:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.5.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatBytesIn:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.6.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPktsOut:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.7.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatBytesOut:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.8.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPersistConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.9.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.10.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatCurConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.11.3.115.103.49.2.2.115.49.80
    axServerPortStatusInServiceGroupMemberStat:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.12.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotalL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.13.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotalCurrL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.14.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatTotalSuccL7Reqs:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.15.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatResponseTime:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.16.3.115.103.49.2.2.115.49.80
    axServiceGroupMemberStatPeakConns:
1.3.6.1.4.1.22610.2.4.3.3.4.1.1.17.3.115.103.49.2.2.115.49.80
```

show snmp stats

Description Displays SNMP statistics or display the statistics based on the output filter.

NOTE: SNMP statistics are also included automatically in show techsupport output.

Syntax

```
show snmp stats
```

Mode All

Example The following command displays SNMP statistics:

```
ACOS#show snmp stats

Bad SNMP version errors                  0
Unknown community name                   0
Illegal operation for community name     0
Encoding Error                           0
Unknown security models                  0
Invalid ID                               0
Input packets                            0
Number of requested variables            0
Get-Request PDUs                         0
Get-Next PDUs                            0
Packets drop                             0
Too big errors                           0
No such name errors                      0
Bad values errors                        0
General errors                           0
Output packets                           0
Get-Response PDUs                        0
SNMP output traps                        0
```

show startup-config

Description Displays a configuration profile or displays a list of all the locally saved configuration profiles.

Syntax

```
show startup-config all
```

Syntax

```
show startup-config
[profile profile-name
  [all-partitions | partition {shared | partition-name}]
]
```

Parameter	Description
profile *profile-name*	Displays the commands that are in the specified configuration profile.
all	Displays a list of the locally stored configuration profiles.
all-partitions	Shows all resources in all partitions. In this case, the resources in the shared partition are listed first. Then the resources in each private partition are listed, organized by partition.
partition {**shared** | *partition-name*}	Shows only the resources in the specified partition.

Mode All

Usage The profile name must be specified before any partition names.

The **all-partitions** and **partition** *partition-name* options are applicable on ACOS Devices that are configured with L3V partitions. If you omit both options, only the resources in the shared partition are shown. (If no partitions are configured, all resources are in the shared partition, so you can omit both options.)

The **all-partitions** option is applicable only to admins with Root, Read-write, or Read-only privileges.

When entered without the **all** or *profile-name* option, this command displays the contents of the configuration profile that is currently linked to “startup-config”. Unless you have relinked “startup-config”, the configuration profile that is displayed is the one that is stored in the image area from which the ACOS Device most recently rebooted.

Example The following example shows how to view the startup-config in partition “companyB” (truncated for brevity):

```
ACOS# show startup-config partition companyB
Show startup-config profile in partition "companyB"
Building configuration...
```

```
!Current configuration: 2442 bytes
!Configuration last updated at 11:23:01 IST Tue Sep 30 2014
!Configuration last saved at 11:31:59 IST Tue Sep 30 2014
!
active-partition companyB
!
  exit
!
!
ip access-list test
  4 remark 123
  exit
!
!
ipv6 access-list test
  4 remark 123
  exit
!
...
```

Example The following example shows the startup-config of the ACL:

```
ACOS(config)(NOLICENSE)#show startup-config
Show default startup-config
Building configuration...
!Current configuration: 615 bytes
!Configuration last updated at 08:06:35 IST Thu Oct 13 2022
!Configuration last saved at 08:08:37 IST Thu Oct 13 2022
!64-bit Advanced Core OS (ACOS) version 6.0.0-d, build 326
(Oct-1-2022,07:53)
!
!
access-list 60 4 deny 5.1.1.1 0.0.0.0
!
access-list 60 20 deny 5.1.1.2 0.0.0.0
!
access-list 160 4 deny ip 6.1.1.1 0.0.0.0 any
!
access-list 160 40 deny ip 6.1.1.2 0.0.0.0 any
!
```

```
ip access-list acl_sample_ipv4
  4 deny ip 7.1.1.1 0.0.0.0 any
  55 deny ip 7.1.1.2 0.0.0.0 any
!
ipv6 access-list acl_sample_ipv6
  4 deny ipv6 68::55:6:78/128 any
  50 deny ipv6 68::55:6:79/128 any
!
```

Related Commands:

- show admin

show statistics

Description Display packet statistics for Ethernet interfaces.

Syntax

```
show statistics [interface  int-typeport-num]
```

Mode All

Example The following command shows brief statistics for all Ethernet interfaces on an ACOS Device:

```
ACOS# show statistics
Port  Good Rcv       Good Sent      Bcast Rcv      Bcast Sent
   Errors
-------------------------------------------------------------------
-------------
1     3026787        3013699        91573          154220
   0
2     0              0              0              0
   0
3     0              0              0              0
   0
...
```

Example The following command shows detailed statistics for Ethernet interface 1:

```
ACOS# show statistics interface ethernet 1
```

```
Port  Link  Dupl Speed     IsTagged  MAC Address
-------------------------------------------------
1     Up    Full 1000      Untagged  0090.0B0A.D860

 Port 1 Counters:
            InPkts             6926           OutPkts
427659
          InOctets           477802         OutOctets
323788182
   InBroadcastPkts             5573  OutBroadcastPkts
62389
   InMulticastPkts                0  OutMulticastPkts
359729
         InBadPkts                0        OutBadPkts
    0
       OutDiscards                0        Collisions
    0
       InLongOctet           477802        InAlignErr
    0
       InLengthErr                0         InOverErr
    0
        InFrameErr                0          InCrcErr
    0
        InNoBufErr                0         InMissErr
   48
      InLongLenErr                0     InShortLenErr
    0
       OutAbortErr                0     OutCarrierErr
    0
        OutFifoErr                0 OutLateCollisions
    0
     InFlowCtrlXon                0    OutFlowCtrlXon
    0
    InFlowCtrlXoff                0   OutFlowCtrlXoff
    0
  InBufAllocFailed                0
     InUtilization               15    OutUtilization
    0
```

show store

Description Display the configured file transfer profiles in the credential store. The credential store is a saved set of access information for file transfer between the ACOS Device and remote file servers.

Syntax `show store [backup | export | import] name`

Mode All

Example The example below shows an example of this command output:

```
ACOS(config)# show store export
Export Store Information
StoreName                          url
         SuccessRate FailedRate
================================================================
==============================
green-export-store
tftp://:****@172.17.3.156/green.txt        0         0
```

show switch

Description Display internal system information from the ASIC registers for troubleshooting.

NOTE: This command is only supported on some A10 Thunder Series devices, and not all parameters are supported on all devices. Use the "?" character to find out whether or not this command is supported on your system, and which parameters are supported.

Mode `show switch {debug | mac-table | vlan-table | xfp-temp}`

Parameter	Description
debug	View debug information.
mac-table	View the MAC addresses configured on the ASIC.
vlan-table	View the VLANs configured on the ASIC.
xfp-temp	View the XFP temperatures.

Mode All

show system app-performance

Description Show application performance data and details.

Syntax

```
show system app-performance [details]
```

Field	Description
details	Use detail option to get per port information. Application performance details for Master and Blade.

Default By default, aggregated information is provided.

Mode All

Usage Use the “detail” option to get per-slot information.

Example The following outputs are displayed.

```
ACOS#show system app-performance
L4cpi       L7cpi       L7tpi       SSLcpi      ServSSLcpi Natcpi
   FWcpi
-------------------------------------------------------------------
---------
0           0           0           0           0          0
   0
```

show system cpu-load-sharing

Description Displays CPU load sharing information.

CPU load sharing can be configured using the system cpu-load-sharing command.

Syntax

```
show system cpu-load-sharing [statistics [detail]]
```

Parameter	Description
statistics	Shows CPU load sharing statistics.
detail	Show per CPU counters.

Mode All

Example The following command shows output from the CPU load sharing feature. In this example, the counter for the “Load Sharing Triggered” field is incremented every time a CPU enters into load-sharing mode. Similarly, the counter for the “Load Sharing Untriggered” field is incremented every time a CPU is subsequently removed from load-sharing mode.

```
ACOS(config)#show system cpu-load-sharing statistics
CPU Load-Sharing Stats
----------------------
Load Sharing Triggered                  1
Load Sharing Untriggered                1
```

Example If the command is used without the **statistics** option, then the output simply displays which CPUs are in load-sharing mode. The example below shows that CPU 1, CPU 2, and CPU 3 are in load-sharing mode.

```
ACOS(config)#show system cpu-load-sharing
CPUs in Load-Sharing Mode: 1 2 3
```

Example The following command shows output from the CPU load sharing feature. In this example, the "Round Robin forward home for L7" field displays the number of L7 session packets forwarded to the home CPU for processing.

```
ACOS(config)#show system cpu-load-sharing statistics
CPU Load-Sharing Stats
----------------------
Load Sharing Triggered                  2
Load Sharing Untriggered                2
Round Robin Pkt Received                2779983
Round Robin Pkt sent(fwd)               0
Round Robin Pkt sent(rev)               0
Round Robin drop for L7                 0
```

```
Round Robin forward home for L7          2779616
Home CPU sent(new conn)                  339
Home CPU sent(existed conn)              2540541
Home CPU sent(queue full drop)           0
```

show system geo-location

Description Show the status of system geo-location mappings.

Syntax

```
show system geo-location
{
[db [geo-location-name]
    [[statistics] ip-range range-start range-end]
    [[statistics] depth num]
    [[statistics] directory num]
    [[statistics] top num [percent [global]]]
    [statistics]]

[file [file-name]]

[ip ipaddr [statistics] [policy policy-name]]
[ipv6 ipv6addr [statistics] [policy policy-name]]
[rdt   [active [geo-location-name ...]
          [site site-name] [depth num]]
```

Parameter	Description
db *[options]*	Displays the geo-location database. If you specify a geo-location name, only the entries for that geo-location are shown. Otherwise, entries for all geo-locations are shown. • **ip-range** – Displays entries for the specified IP address range. • **depth** *num* – Specifies how many nodes within the geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify depth 2. By default, the full tree (all nodes) is displayed. • **directory** *num* – Displays entries for the specific geo-location database directory. • **top** *num* [**percent** [**global**]] – Display the top

Parameter	Description
	statistics for the selected geo-location database. • **statistics** – Displays client statistics for the specified geo-location.
file [*file-name*]	Displays the geo-location database files on the ACOS Device, and their load status. (Data from a geo-location database file does not enter the geo-location database until you load the file.
ip *ipaddr*	Displays geo-location database entries for the specified IP address. • **statistics** – Displays client statistics for the specified geo-location. • **policy** *policy-name* – Filter output by policy.
ipv6 *ipv6addr*	Displays geo-location database entries for the specified IPv6 address. • **statistics** – Displays client statistics for the specified geo-location. • **policy** *policy-name* – Filter output by policy.
rdt [*options*]	Displays aRDT data for geo-locations. You can use the following options: • **active** – Displays data for aRDT. • *geo-location-name* – Displays aRDT data only for the specified GSLB geo-location. • **site** *site-name* – Displays aRDT data only for the specified GSLB site. • **depth** *num* – Specifies how many nodes within the geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify **depth 2**. By default, the full tree (all nodes) is displayed.

Mode All

Usage The matched client IP address and the hits counter indicate the working status of the geo-location configuration.

```
The following command shows the status of a geo-location db
named “pc”:
ACOS# show system geo-location db arin
                  Last = Last Matched Client, Hits = Count of
Client matched
                  Sub = Count of Sub Geo-location
                  T = Type, P-Name = Policy name
                    G(global)/P(policy), S(sub)/R(sub range)
                    M(manually config)/B(built-in)

Geo-location: arin
From            To/Mask         Last            Hits      Sub
T    P-Name
-------------------------------------------------------------------
----------
                                                0         21
G
```

Example The following table describes the fields in the command output:

Field	Description
Geo-location	Name of the geo-location.
From	Beginning address in the address range assigned to the geo-location.
To	Ending address in the address range assigned to the geo-location.
Last	Client IP address that most recently matched the geo-location. If the value is “empty”, no client addresses have matched.
Hits	Total number of client IP addresses that have matched the geo-location.
Sub	Number of sublocations within the geo-location. For example, if you configure the following geo-locations,

Field	Description
	geo-location “pc” has two sublocations, “pc.office” and “pc.lab”. geo-location pc 10.1.0.0 mask /16 geo-location pc.office 10.1.1.0 mask /24 geo-location pc.lab 10.1.2.0 mask /24
T	Type of geo-location: G – The geo-location is configured at the global level in the ACOS Device configuration. P – The geo-location is configured within a system or firewall policy.
P-Name	Name of the policy where the geo-location is configured.

Example The following command shows the load status information for a geo-location database file:

```
ACOS(config)# show system geo-location file test1
                T = T(Template)/B(Built-in), Per = Percentage
of loading
Filename                T Template               Per  Lines
Success  Error
-------------------------------------------------------------
----------
test1                   T t1                     98%  11
10       0
```

Example The following command displays entries in the geo-location database:

```
ACOS(config)# show system geo-location db

                 Last = Last Matched Client, Hits = Count of
Client matched
                 T = Type, Sub = Count of Sub Geo-location
                     G(global)/P(policy), S(sub)/R(sub range)
                     M(manually config)
```

```
Global
Name            From            To/Mask         Last
Hits      Sub   T
-------------------------------------------------------------------
-----------
NA              (empty)         (empty)         (empty)
0         1     G

Geo-location: NA, Global
Name            From            To/Mask         Last
Hits      Sub   T
-------------------------------------------------------------------
-----------
US              (empty)         (empty)         (empty)
0         10    GS

Geo-location: NA.US, Global
Name            From            To/Mask         Last
Hits      Sub   T
-------------------------------------------------------------------
----------
                69.26.125.0     69.26.125.255   (empty)
0         0     GR
                69.26.126.0     69.26.126.255   (empty)
0         0     GR
                69.26.127.0     69.26.127.255   (empty)
0         0     GR
...
```

Related Commands:

- gslb system geo-location load

show system ip-threat-list

Description Displays the IP threat list entries. For more information, see *Firewall Configuration* guide .

Syntax

```
show system ip-threat-list entries { ipv4_addr | ipv6_addr }
```

Mode All

Example The following command shows the IP threat list information:

```
ACOS# show system ip-threat-list entries 192.168.1.1
IP Address  Match Type  In-SPE  Age
-----------------------------------
192.168.1.1 Source 0 5
```

The following table describes the fields in the command output:

Parameter	Description
IP Address	The IP address which is dropped.
Match Type	This field indicates the match type . It can have one of the following values: • Source • Dest • Internet-Host
In-SPE	This flag indicates if the Security Policy Engine (SPE) has dropped the packet in hardware. This functionality is not supported for all devices.
Age	Number of minutes the entry remains in the table before being removed.

show system inuse-rxtx-desc-info

Description Displays the number of RxTx descriptor size that are currently used by ACOS per queue.

This command is used in Baremetal, and vThunder platforms, which support different types of network interfaces (nic) and virtual nics.

Syntax

```
show system inuse-rxtx-desc-info
```

Mode All

Example The following command shows the RxTx descriptor information that are in use:

```
ACOS# show system inuse-rxtx-desc-info
Port-Num   RxD-Size   TxD-Size  Rx-Queues  Tx-Queues
-------------------------------------------------------------------
-----
1            512        512          1          1
2            512        512          1          1
3            512        512          1          1
4            512        512          1          1
```

show system inuse-rxtx-queue-info

Description Displays the port received data (Rx) and transmitted data (Tx) descriptor or queue information that are in use.

Syntax

```
show system inuse-rxtx-queue-info
```

Mode All

Example The following command shows the RxTx queues information that are in use:

```
ACOS# show system inuse-rxtx-queue-info
Port-Num   RxD-Size   TxD-Size  Rx-Queues  Tx-Queues
-------------------------------------------------------------------
-----
1            512        512          1          1
2            512        512          1          1
3            512        512          1          1
4            512        512          1          1
```

show system job-offload statistics

Description Displays number of jobs and the different transition or errors within the CPU Offload Infrastructure.

Syntax

```
show system job-offload [statistics]
```

Mode All

Example The example example statistics.

```
(config)#show system job-offload statistics
Total
-----------------------------------------
Jobs                                0
Jobs Submitted                      0
Jobs Received                       0
Jobs Executed                       0
Jobs Sent Back Home                 0
Jobs Received Home                  0
Jobs Completed                      0
Jobs Failed to Submit               0
No More Space in Q                  0
Failed to Execute Job               0
Failed to Complete Job              0
```

The following table describes the statistics displayed in the output:

Parameter	Description
Jobs	Number of jobs that are currently executed.
Jobs Submitted	Number of jobs submitted into the infrastructure.
Jobs Received	Number received by the offload CPU.
Jobs Executed	Number of jobs that were successfully executed on the offload CPU (called the data callback).
Jobs Sent Back Home	Number of jobs submitted onto the home CPU response queue.
Jobs Received Home	Number of jobs received by the home CPU.
Jobs Completed	Number of jobs successfully completed (called the finish callback).
Jobs Failed	Number of jobs that were failed to submit.

Parameter	Description
to Submit	This could be either due to no more space or out of memory issues.
No More Space in Q	Number of jobs failed to queue due to lack of space. This also accounts for multiple queues.
Failed to Execute Job	Number of jobs (data callback) failed to execute.
Failed to Complete Job	Number of jobs (finish callback) failed to complete.

show system link-monitor-polling-info

Description Displays the link monitor task configuration on system and ports.

Syntax

```
show system link-monitor-polling-info
```

Mode All

Example The following command shows the link monitor polling information.

```
ACOS# show system link-monitor-polling-info
Link Monitor Polling : Enabled
Per-port Link Monitor Polling information:
-----------------------------------------
Port-Num  Link Monitor Polling Status
-----------------------------------------
1                    Y
2                    Y
3                    Y
4                    Y
```

show system management-interface-mode

Description Displays the status of no separate management interface mode, if selected.

This command is supported in case of vThunder or ESXI virtual platform, where the data interface is used as management interface itself.

Syntax

```
show system management-interface-mode
```

Mode All

Example The following command shows the configured management interface:

```
ACOS# show system management-interface-mode
```

show system platform

Description Displays platform-related information and statistics.

Syntax

```
show system platform
{buffer-stats |
 cpu-packet-statistics |
 busy-counter |
 interface-stats |
 statistics |
 te-mac
}
```

Parameter	Description
`buffer-stats`	Shows counters for buffer statistics.
`cpu-packet-statistics`	Shows per-CPU packet statistics.
`busy-counter`	Shows counters for system busy statistics.
`interface-stats`	Shows counters for interface statistics.
`statistics`	Shows counters for internal statistics.
`te-mac`	Shows the Traffic Engineering (TE) MAC address on Multi-PU platforms.

Mode All

Example The following command shows platform buffer statistics:

```
ACOS# show system platform buffer-stats
Buffers available in various states/threads...
-------------------------------------------------
Thread       Cache         App    AppQueue        Misc
-------------------------------------------------
Q0             5015           0           0           0
Q1             8629           0           0           0
Approximate # buffers in App      0
Approximate # buffers in App_cp   0
Approximate # buffers in Cache_cp 4094
Approximate # buffers in Cache    13644
Approximate # buffers in thread Q 0
Approximate # buffers in dcmsg Q  0
Approximate # buffers in misc     0
Approximate # buffers in dfree    0
Approximate # buffers free        819599
Approximate # buffers avail in HW 815505
Approximate # buffers in total    833243
```

Example The following command shows the TE MAC address. This command is supported only on the Multi-PU platforms and when VRRP-A is not enabled.

```
ACOS# show system platform te-mac
Inside MAC : 001f.a008.7fc3
Outside MAC : 001f.a008.7fc2
```

show system path

Description Show the statistics of system path status for layer 2 health monitoring.

Syntax `show system path {summary | details}`

Parameter	Description
summary	Displays the summary of the system path status.
details	Displays the details of the system path status.

Mode All

The following table describes the fields in the command output.

Field	Description
L2HM Path/Path	Displays the name of the layer 2 health monitoring path object.
Health-Check	Displays the name of the health check object.
Path-State	Displays the state of the path. It could be either UP or DOWN.
Apps (Instances)	Displays the application or real server instance.
Interface-1 Interface-2	Displays the endpoints interface.

Example The following command displays the summary of the system path status.

```
ACOS(config)# show system path summary
L2HM Path       Health-Check       Path-State     Apps
(Instances)
Ssli-path-1     HC-Obj             UP             SLB(1)
Ssli-path-2     HC-Obj             UP
```

Example The following command displays the details of the system path status.

```
ACOS(config)# show system path details
Path         : Ssli-path-1
Interface-1 : trunk-1
Interface-2 : trunk-2
Health-Check: HC-Obj
Path-State   : UP
Apps         : SLB(1)
Path         : Ssli-path-2
Interface-1 : eth-2
Interface-2 : eth-3
Health-Check: HC-Obj
Path-State   : UP
```

```
Apps         :
```

show system port-list

Description Displays the physical and logical ports available on the system.

Syntax

```
show system port-list
```

Mode All

Example The following sample show command shows:

```
ACOS# show system port-list
Port-IDX  Port-Num  Status  MAC-Addr           Max-Speed  Node
 PCI-Addr
0         1         +       00:1f:a0:23:c6:32  1000       0
 02:00.0
1         2         +       00:1f:a0:23:c6:33  1000       0
 02:00.1
2         3         +       00:1f:a0:23:c6:34  1000       0
 02:00.2
3         4         +       00:1f:a0:23:c6:35  1000       0
 02:00.3
4         7         +       00:1f:a0:23:c6:38  1000       0
 03:00.0
5         8         +       00:1f:a0:23:c6:39  1000       0
 03:00.1
6         5         +       00:1f:a0:23:c6:36  1000       0
 03:00.2
7         6         +       00:1f:a0:23:c6:37  1000       0
 03:00.3
8         M         +       00:1f:a0:23:c6:3a  40000      0
 17:00.0
9         17        +       00:1f:a0:23:c6:3e  40000      0
 17:00.1
10        18        +       00:1f:a0:23:c6:3f  40000      0
 17:00.2
11        19        +       00:1f:a0:23:c6:40  40000      0
 17:00.3
```

```
12          20          +         00:1f:a0:23:c6:44   40000       0
 18:00.0
13          15          +         00:1f:a0:23:c6:41   25000       0
 65:00.0
14          16          +         00:1f:a0:23:c6:42   25000       0
 65:00.1
15          13          +         00:1f:a0:23:c6:3f   25000       0
 66:00.0
16          14          +         00:1f:a0:23:c6:41   25000       0
 66:00.1
17          9           +         00:1f:a0:23:c6:3a   10000       0
 b7:00.0
18          10          +         00:1f:a0:23:c6:3b   10000       0
 b7:00.1
19          11          +         00:1f:a0:23:c6:3c   10000       0
 b7:00.2
20          12          +         00:1f:a0:23:c6:3d   10000       0
 b7:00.3
```

The following table describes the fields in the command output:

Parameter	Description
Port-IDX	The internal index used by ACOS to reference the port within the database.
Port-Num	The logical port number used in the ACOS configuration.
Status	The status of the port. + means the port is active and the link is up. other (- or blank) means the port is down or disabled.
MAC-Addr	The unique MAC address assigned to the port/interface.
Max-Speed	The maximum supported link speed (in Mbps) of the port (for example, 1000 = 1Gbps, 40000 = 40Gbps).

Parameter	Description
Node	The node or chassis number (in multi-node systems, usually 0 for single node).
PCI-Addr	The PCI address of the network interface card (NIC) or port in the format `Bus:Device.Function`. This maps the port to its physical hardware on the PCI bus.

show system radius server

Description Show configuration information or statistics for the ACOS RADIUS server.

Syntax

```
show system radius server {config | statistics}
```

Parameter	Description
config	Displays the configuration for the ACOS RADIUS server.
statistics	Displays statistics for the ACOS RADIUS server.

Mode All

Example The following command displays RADIUS server statistics:

```
ACOS# show system radius server statistics
LSN RADIUS Server Statistics:
-----------------------------------------
MSISDN Received                0
IMEI Received                  0
IMSI Received                  0
Custom Attribute Received      0
RADIUS Request Received        0
RADIUS Request Dropped         0
RADIUS Request Bad Secret Dropped 0
RADIUS Request No Key Attribute Dropped 0
RADIUS Request Malformed Dropped 0
RADIUS Request Ignored         0
```

```
RADIUS Request Table Full Dropped 0
RADIUS Secret Not Configured Dropped 0
HA Standby Dropped              0
Framed IPV6 Prefix Length Mismatch 0
```

The following table describes the fields in this command's output.

Field	Description
MSISDN Received	Number of MSISDN attributes received.
IMEI Received	Number of IMEI attributes received.
IMSI Received	Number of IMSI attributes received.
Custom attribute Received	Number of custom attributes received.
RADIUS Request Received	Number of Accounting Requests received.
RADIUS Request Dropped	Number of Accounting Requests dropped.
RADIUS Request Bad Secret Dropped	Number of Accounting Requests dropped due to bad secret.
RADIUS Request No Key Attribute Dropped	Number of Accounting Requests dropped due to no key attribute.
RADIUS Request Malformed Dropped	Number of Accounting Requests dropped due to packet format errors or shared secret errors.
RADIUS Request Ignored	Number of Accounting Requests ignored.
RADIUS Request Table Full Dropped	Number of Accounting Requests dropped due to capacity constraints.
RADIUS Secret Not Configured Dropped	Number of Accounting Requests dropped due to secret not configured.
HA Standby Dropped	Number of Accounting Requests dropped due to high availability standby state.
Framed IPv6 Prefix Length Mismatch	Number of Accounting Requests dropped due to mismatch Framed IPv6 Prefix.

show system radius table

Description Show the RADIUS accounting information stored on the ACOS device.

Syntax

```
show system radius table
[
brief |
imei string |
imsi string |
inside-ip ipaddr |
msisdn string |
custom-attr-name [starts-with] string [case-insensitive]
]
```

Parameter	Description
brief	Shows statistics only.
imei *string*	Shows entries only for IMEI numbers.
imsi *string*	Shows entries only for IMSI numbers.
inside-ip *ipaddr*	Shows entries only for inside IP addresses.
msisdn *string*	Shows entries only for MSIDSN numbers.
custom-attr-name [**starts-with**] *string* [**case-insensitive**]	Shows entries only for the specified custom attribute. To filter based on the beginning portion of the attribute name, use the **starts-with** option. The **case-insensitive** option ignores the distinction between uppercase and lower case characters in the string.

Mode All

Example The following command shows the RADIUS server table for CGN:

```
ACOS# show system radius table
LSN RADIUS Table Statistics:
-------------------------------------------
Record Created                  1
Record Deleted                  0

MSISDN           IMEI               IMSI             Inside-IP
```

```
------------------------------------------------------------
-------------
012345678133     20123456789111     101234567
10.10.10.1
Total RADIUS Records Shown: 1
```

The following table describes the fields in this command's output.

Field	Description
Record Created	Number of records created.
Record Deleted	Number of records deleted.
MSISDN	MSISDN field of the record.
IMEI	IMEI field of the record.
IMSI	IMSI field of the record.
Inside-IP	Inside client IP associated with this record.

show system rxtx-desc-info

Description Displays the port received data (Rx) and transmitted data (Tx) descriptor configured for the queue.

Syntax

```
show system rxtx-desc-info
```

Mode All

Example The following command shows the RxTx descriptor information:

```
ACOS# show system rxtx-desc-info
Port-IDX   Port-Num   RxD-Size   TxD-Size  Rx-Queues  Tx-
Queues
------------------------------------------------------------
-----
0          M             0          0          0          0
1          1             0          0          0          0
2          2             0          0          0          0
3          3             0          0          0          0
4          4             0          0          0          0
```

show system rxtx-queue-info

Description Displays the port received data (Rx) and transmitted data (Tx) descriptor or queue information.

Syntax

```
show system rxtx-queue-info
```

Mode All

Example The following command shows the RxTx queues information:

```
ACOS# show system rxtx-queue-info
Port-IDX   Port-Num   RxD-Size   TxD-Size  Rx-Queues  Tx-
Queues
-------------------------------------------------------------------
-----
0          M             0          0          0          0
1          1             0          0          0          0
2          2             0          0          0          0
3          3             0          0          0          0
4          4             0          0          0          0
```

show system resource-usage

Description Display the minimum and maximum numbers of system resources that can be configured or used, the default maximum number allowed by the configuration, and the number currently in use.

For example, the “l4-session-count” row of the output shows the number of Layer 4 sessions that are currently in use, as well as the maximum number currently supported by the configuration (the default maximum), and the range of values that can be assigned to the default maximum.

In general, if a resource listed in the output has the same value in the Current and Maximum columns (GSLB resources, for example), then the allocation for that resource can not be changed.

Syntax

```
show system resource-usage [template [default | template-
name]]
```

Mode All

Usage To change system resource usage settings, use the system resource-usage command.

You must reload or reboot the system after making changes to system resource-usage settings in order to place the changes into effect. For most system resource-usage settings, a reload is sufficient. However, a change to the l4-session-count setting requires a reboot.

If the target device is not reloaded, the system resource-usage settings synchronized from the active device appear in the standby device's running-config, but do not actually take effect until the reload or reboot.

- If you manually synchronize the configuration, you have the option to reload the target device immediately following the synchronization. If you do not use this option, you can reload the device later.
- If you are using VRRP-A in combination with aVCS, configuration synchronization is automatic. In this case, you must reload or reboot the target device to place the system resource-usage changes into effect.

NOTE: The target device is not automatically reloaded following configuration synchronization.

Example Below is a sample output for this command.

```
ACOS# show system resource-usage
Resource                              Current    Default
Minimum    Maximum
-------------------------------------------------------------
----------------
l4-session-count                      2097152    2097152
262144     16777216
nat-pool-addr-count                   10         10         10
       2000
class-list-ipv6-addr-count            524288     524288
524288     1048576
```

```
class-list-ac-entry-count              65536       65536
65536       131072
auth-portal-html-file-size             20          20          4
      120
auth-portal-image-file-size            6           6           1
      80
max-aflex-file-size                    32          32          16
      256
aflex-table-entry-count                102400      102400
102400      1010000
max-aflex-authz-collection-number      512         512         256
      4096
radius-table-size                      1000000     1000000
500000      1000000
monitored-entity-count                 1204        1204        640
      18336
authz-policy-number                    128         128         32
      2000
ram-cache-memory-limit                 2048        2048        512
      2048
ipsec-sa-number                        2000        2000        8
      2000
auth-session-count                     104856      104856
10485       104856
class-list-entry-count                 65536       65536
65536       2097152
```

The following table describes the fields in this output for each resource.

Field	Description
Current	Number of resources.
Default	Default number of maximum resources that can be configured based on the current configuration.
Minimum	Minimum number of resources that can be configured.
Maximum	Maximum number of resources that can be

Field	Description
	configured.
l4-session-count	Layer 4 sessions supported. The range is platform specific.
nat-pool-addr-count	Total number of NAT pool addresses available for configuration in the system. The range is platform specific.
class-list-ipv6-addr-count	The IPv6 addresses allowed within each IPv6 class list.
class-list-ac-entry-count	The SNI entries allowed per ACOS device for Aho-Corasik class-lists.
auth-portal-html-file-size	The file size allowed for AAM HTML files.
auth-portal-image-file-size	The file size allowed for AAM portal image files.
max-aflex-file-size	The size of an aFleX script in Kbytes.
aflex-table-entry-count	The number of configurable aFlex table entries in the system.
max-aflex-authz-collection-number	The number of collections supported by aFleX authorization.
radius-table-size	The total number of con-figurable CGNV6 RADIUS table entries.
monitored-entity-count	The number of monitored entities for visibility.
authz-policy-number	Number of authorization policies allowed.
ram-cache-memory-limit	The memory used by the RAM cache.
ipsec-sa-num-	The number of IPsec SAs allowed.

Field	Description
ber	
auth-session-count	The total number of AAM session.
class-list-entry-count	The total number of class lists that the platform will support. The value depends on the platform.

show system shared-poll-mode

Description Displays the shared poll mode status. The system shared-poll-mode command enables or disables the mode.

Syntax

```
show system shared-control-mode
```

Mode All

Usage To change system resource usage settings, use the system shared-poll-mode command.

Example Below is a sample output for this command.

```
A2# show system shared-poll-mode
Shared poll mode is enabled
A2#
```

show system table-integrity

Description Show table integrity for IPv4/IPv6 FIB, ARP, ND6, and MAC tables.

Syntax

```
show system table-integrity
```

Mode All

Example Below is a sample output for this command.

```
ACOS# show system table-integrity?
table-integrity Table integrity for IPv4/v6 FIB, ARP, ND6 and
MAC
```

show system table-integrity statistics

Description Show system table integrity statistics.

Syntax

```
show system table-integrity statistics [ detail | arp-table
[detail] | ipv4-fib-table [detail] | ipv6-fib-table [detail] |
mac-table [detail] | nd6-table [detail] ]
```

Mode All

Example Below is a sample output for this command.

```
ACOS# show system table-integrity statistics
 ================ARP-TABLE=========================
 =============PU1=============
Total table synchronization sent:       1
Total table checksum sent:              26
Total table checksum canceled:          0
===T0-synchronization===
Start time:                             Friday, April 09, 2021
06:42:13
Number of entries sent:                 2
End time:                               Friday, April 09, 2021
06:42:13
=============PU2=============
Total table synchronization received:   1
Total table checksum received:          26
Total table checksum mismatch:          1
===T0-synchronization===
Start time:                             Friday, April 09, 2021
06:42:13
Number of entries received              2
Number of entries added:                0
Number of entries removed:              11
End time:                               Friday, April 09, 2021
06:42:16

================ND6-TABLE====================
=============PU1======================
Total table synchronization sent:       0
Total table checksum sent:              16
```

```
Total table checksum canceled:          0
=============PU2=======================
Total table synchronization received:   0
Total table checksum received:          16
Total table checksum received:          16
Total table checksum mismatch:          0

================IPV4-FIB-TABLE==================
=============PU1====================
Total table synchronization sent:       0
Total table checksum sent:              0
Total table checksum canceled:          0
=============PU2=============
Total table synchronization received:   0
otal table checksum received:          0
Total table checksum received:          0
Total table checksum mismatch:          0

================IPV6-FIB-TABLE================
=============PU1====================
Total table synchronization sent:       0
Total table checksum sent:              0
Total table checksum canceled:          0
=============PU2=============
Total table synchronization received:   0
Total table checksum received:          0
Total table checksum received:          0
Total table checksum mismatch:          0

================MAC-TABLE================
=============PU1=============
Total table synchronization sent:       0
Total table checksum sent:              22
Total table checksum canceled:          0
=============PU2=============
Total table synchronization received:   0
Total table checksum received:          22
Total table checksum received:          22
Total table checksum mismatch:          0
```

Field	Description
ARP-TABLE	ARP table integrity statistics counters.
ND6-TABLE	ND6 table integrity statistics counters.
IPv4-FIB-TABLE	IPv4-FIB table integrity statistics counters.
IPv6-FIB-TABLE	IPv6-FIB table integrity statistics counters.
MAC-TABLE	MAC table integrity statistics counters.

Example View detailed information of table integrity statistics counters.

```
ACOS# show system table-integrity statistics detail

 ================ARP-TABLE================
=============PU1=============
Total table synchronization sent:       2
Total table checksum sent:              29
Total table checksum canceled:          0
===T0-synchronization===
Start time:                             Friday, April 09, 2021
06:45:33
Number of entries sent:                 13
End time:                               Friday, April 09, 2021
06:45:33
===T-1 synchronization===
Start time:                             Friday, April 09, 2021
06:42:13
Number of entries sent:                 2
End time:                               Friday, April 09, 2021
06:42:13
=============PU2=============
Total table synchronization received:   2
Total table checksum received:          29
Total table checksum mismatch:          2
===T0-synchronization===
Start time:                             Friday, April 09, 2021
06:45:33
Number of entries received              13
```

```
Number of entries added:                11
Number of entries removed:              0
End time:                               Friday, April 09, 2021
06:45:36
===T-1 synchronization===
Start time:                             Friday, April 09, 2021
06:42:13
Number of entries received              2
Number of entries added:                0
Number of entries removed:              11
End time:                               Friday, April 09, 2021
06:42:16

================ND6-TABLE================
=============PU1=============
Total table synchronization sent:       0
Total table checksum sent:              16
Total table checksum canceled:          0
=============PU2=============
Total table synchronization received:   0
Total table checksum received:          16
Total table checksum received:          16
Total table checksum mismatch:          0

================IPV4-FIB-TABLE================
=============PU1=============
Total table synchronization sent:       0
Total table checksum sent:              0
Total table checksum canceled:          0
=============PU2=============
Total table synchronization received:   0
Total table checksum received:          0
Total table checksum received:          0
Total table checksum mismatch:          0

================IPV6-FIB-TABLE================
=============PU1=============
Total table synchronization sent:       0
Total table checksum sent:              0
Total table checksum canceled:          0
```

```
============PU2=============
Total table synchronization received:   0
Total table checksum received:          0
Total table checksum received:          0
Total table checksum mismatch:          0

================MAC-TABLE=================
============PU1=============
Total table synchronization sent:       0
Total table checksum sent:              23
Total table checksum canceled:          0
============PU2=============
Total table synchronization received:   0
Total table checksum received:          23
Total table checksum received:          23
Total table checksum mismatch:          0
```

show system tcp rate-limit-reset-unknown-conn

Description Show TCP reset packet rate limit statistics.

Syntax

```
show system tcp rate-limit-reset-unknown-conn
```

Mode All

Example Below is a sample output for this command.

```
ACOS# show system tcp rate-limit-reset-unknown-conn
Rate limit for unknown-reset-conn:
--------------------------------------------------
Rate limit                                      2
Current rate                                    0
Rate limit drops                                1443940083
```

Field	Description
Rate limit	Configured rate limit threshold value per second.
Current rate	Current rate of unknown connection reset.

Field	Description
Rate limit drops	Total number of unknown connection reset dropped by rate limit.

show system-ssl status

Description Display system SSL status.

Syntax

```
show system-ssl status [detail]
```

Mode All

Usage For per-slot SSL status information, use “detail” option.

Example The following command displays system-ssl status:

```
ACOS# show system-ssl status
HW offload SSL Engine Status
----------------------------------------
SSL Engine-Status                       : Initialized
SSL Engine-Setup                        : Chip(s) are Up
Total SSL Chips in the system           : 3
Number of AEs per Chip                  : 10
Crypto offload support                  : On
```

show tacacs-server

Description Display TACACS statistics.

NOTE: To view the TACACS+ server statistics you must run the command on the shared partition. If you execute this command on the L3V partition, the TACACS+ statistics will not be displayed.

Syntax

```
show tacacs-server [hostname | ipaddr]
```

Parameter	Description
hostname	Only display information for the server with the

Parameter	Description
	specified host name.
ipaddr	Only display information for the server with the specified IP address.

Mode All

Usage This command is available at all configuration levels, but the option to view information for a specified server is only available at Global configuration mode or higher.

Example The following command shows information for TACACS server 5.5.5.5:

```
ACOS# show tacacs-server 5.5.5.5
TACACS+ server              :  5.5.5.5:49
               Socket opens:              0
              Socket closes:              0
              Socket aborts:              0
              Socket errors:              0
            Socket timeouts:              0
   Failed connect attempts:               0
         Total packets recv:              0
         Total packets send:              0
```

show techsupport

Description Displays or exports system information for use when troubleshooting.

Syntax

```
show techsupport [export [use-mgmt-port] url] [page]
```

Option	Description
export	Exports the output to a remote server.
use-mgmt-port	Uses the management port to perform the export.
url	Specify the file transfer protocol, username (if required), and directory path.

Option	Description
	You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: • **tftp://***host***/***file* • **ftp://**[*user@*]*host*[*:port*]**/***file* • **scp://**[*user@*]*host***/***file* • **sftp://**[*user@*]*host***/***file*
page	Shows the information page by page. If this option is not specified, then all the command's output is sent to the terminal at once.

Mode Privileged EXEC level and configuration levels

Example Below is an example of the output for this command using the **page** option:

```
ACOS# show techsupport page

============= Clock Info <Jul 05 2023 07:28:18.032735>
=============
*08:28:18 IST Wed Jul 5 2023

============= Version Info <Jul 05 2023 07:28:18.033426>
=============
Thunder Series Unified Application Service Gateway vThunder
Copyright 2007-2023 by A10 Networks, Inc.  All A10 Networks
products are
protected by one or more of the following US patents:
10749904, 10742559, 10735267, 10708150, 10686683, 10659354,
10637717
10630784, 0623992,  RE47924,  10601788, 10599680, 10594600,
10581976
```

```
10581907, 10554517, 10536517, 10536481, 10530847, 10523748,
10516730
10516577, 10505984, 10505964, 10491523, 10484465, 10469594,
10454844
10447775, 10411956, 10397270, 10389835, 10389538, 10382562,
10360365
10348631, 10341427, 10341335, 10341118, 10334030, 10318288,
10305904
10305859, 10298457, 10268467, 10257101, 10250629, 10250475,
10243791
RE47296,  10230770, 10187423, 10187377, 10178165, 10158627,
10129122
10116634, 10110429, 10091237, 10069946, 10063591, 10044582,
10038693
10027761, 10021174, 10020979, 10002141, 9992229,  9992107,
9986061
9979801, 9979665, 9961136, 9961135, 9961130, 9960967, 9954899,
9954868
9942162, 9942152, 9912555, 9912538, 9906591, 9906422, 9900343,
9900252
9860271, 9848013, 9843599, 9843521, 9843484, 9838472, 9838425,
9838423
9825943, 9806943, 9787581, 9756071, 9742879, 9722918, 9712493,
9705800
9661026, 9621575, 9609052, 9602442, 9596286, 9596134, 9584318,
9544364
9537886, 9531846, 9497201, 9477563, 9398011, 9386088, 9356910,
9350744
9344456, 9344421, 9338225, 9294503, 9294467, 9270774, 9270705,
9258332
9253152, 9231915, 9219751, 9215275, 9154584, 9154577, 9124550,
9122853
9118620, 9118618, 9106561, 9094364, 9060003, 9032502, 8977749,
8943577
8918857, 8914871, 8904512, 8897154, 8868765, 8849938, 8826372,
8813180
8782751, 8782221, RE44701, 8595819, 8595791, 8595383, 8584199,
8464333
```

```
8423676, 8387128, 8332925, 8312507, 8291487, 8266235, 8151322,
8079077
7979585, 7804956, 7716378, 7665138, 7675854, 7647635, 7627672,
7596695
7577833, 7552126, 7392241, 7236491, 7139267, 6748084, 6658114,
6535516
6363075, 6324286, 8392563, 8103770, 7831712, 7606912, 7346695,
7287084
6970933, 6473802, 6374300

64-bit Advanced Core OS (ACOS) version 6.0.1, build 145 (Jun-
28-2023,05:16)
Booted from Hard Disk secondary image
Serial Number:
vThunderBC6120D6EABDDA8DA5EFDA1885D954BE10C68094
aFleX version: 2.0.0
aXAPI version: 3.0
Hard Disk primary image version 6.0.1, build 122
Hard Disk secondary image (default) version 6.0.1, build 145
Last configuration saved at Jun-28-2023, 09:39
Virtualization type: VMware
System Polling Mode : On
Build Type: non-PGO build
Hardware: 4 CPUs(Stepping 1), Single 32G Hard disk
Memory 8127 Mbyte, Free Memory 3433 Mbyte
Hardware Manufacturing Code: N/A
Hotfixes Applied below: HF-ACOS-16
Current time is Jul-5-2023, 08:28
The system has been up 6 days, 22 hours, 46 minutes
--MORE--
```

Related Commands:

- techreport

show terminal

Description Show the terminal settings.

Syntax

```
show terminal
```

Mode All

Example The following command shows the terminal settings.

```
ACOS#show terminal
Idle-timeout is 00:59:00
Length: 32 lines, Width: 90 columns
Editing is enabled
History is enabled, history size is 256
Auto size is enabled
Terminal monitor is off
Terminal prompt format: hostname
Command timestamp format: none
```

show tftp

Description Display the currently configured TFTP block size.

Syntax

```
show tftp
```

Mode All

Example The following command shows the TFTP block size.

```
ACOS(config)# show tftp
TFTP client block size is set to 512
```

show trunk

Description Shows information about a trunk group.

Syntax

```
show trunk num
```

Replace *num* with the trunk number

Mode All

Example The following command shows information for trunk group 1:

```
ACOS# show trunk 1
Trunk ID          : 1       Member Count: 2
Trunk Name        : None
```

```
Trunk Status      : Up
Trunk Type        : Static
Members           : 2    3
Cfg Status        : Enb Enb
Oper Status       : Up  Up
Ports-Threshold   : 6        Timer: 10 sec(s) Running: No
Working Lead      : 1
```

The following table describes the fields in the command output.

Field	Description
Trunk ID	ID assigned to the trunk by the admin who configured it.
Member Count	Number of ports in the trunk.
Trunk Name	Name of the trunk.
Trunk Status	Indicates whether the trunk is up.
Trunk Type	Indicates the trunk type. It can be Static or Link Aggregation Control Protocol (LACP).
Members	Port numbers in the trunk.
Cfg Status	Configuration status of the port.
Oper Status	Operational status of the port.
Ports-Threshold	Indicates the minimum number of ports that must be up for the trunk to remain up. When the number of UP ports falls before the configured threshold, ACOS disables the trunk's member ports and the "show trunk" output displays "Cfg status" as "disabled" (Dis). The ACOS device generates a log message and an SNMP trap if these ports are enabled.
Timer	Indicates the period (seconds) the ACOS device waits before marking a trunk down again during recovery. Default is ten seconds

Field	Description
	When a trunk disabled by ports-threshold is enabled by a CLI command while an insufficient number of trunk members are UP to meet the port threshold requirement, the ACOS device waits the period configured by this option. If the minimum number of ports are still not UP when the timer expires, ACOS device marks the trunk down again.
Running	Indicates whether the ports-threshold timer is currently running. When the timer is running, a port has gone down but the state change has not yet been applied to the trunk's state.
Working Lead	Port number used for responding to ARP requests. **NOTE:** If the lead port is shown as 0 or "None", the trunk interface is down.

show tsig

Description Display the Transaction Signature (TSIG) key files.

TSIG keys provide an additional layer of security for AXFR transactions.

Syntax

```
show tsig
```

Mode All

Example

```
ACOS(config)# show tsig
Name
----------------------------------------
Krpz.com.+157+20696.key
Krpz.com.+157+20696.private
```

```
Total TSIG number: 2
```

show version

Description Display software, hardware, and firmware version information.

Syntax

```
show version [detail | [begin | include | exclude | section]]
LINE
```

Mode All

Example Below is sample output for this command.

```
ACOS# show version
Thunder Series Unified Application Service Gateway TH7650
Copyright 2007-2023 by A10 Networks, Inc.  All A10 Networks
products are
protected by one or more of the following US patents:
10749904, 10742559, 10735267, 10708150, 10686683, 10659354,
10637717
10630784, 0623992,  RE47924,  10601788, 10599680, 10594600,
10581976
10581907, 10554517, 10536517, 10536481, 10530847, 10523748,
10516730
10516577, 10505984, 10505964, 10491523, 10484465, 10469594,
10454844
10447775, 10411956, 10397270, 10389835, 10389538, 10382562,
10360365
10348631, 10341427, 10341335, 10341118, 10334030, 10318288,
10305904
10305859, 10298457, 10268467, 10257101, 10250629, 10250475,
10243791
RE47296,  10230770, 10187423, 10187377, 10178165, 10158627,
10129122
10116634, 10110429, 10091237, 10069946, 10063591, 10044582,
10038693
10027761, 10021174, 10020979, 10002141, 9992229,  9992107,
9986061
9979801, 9979665, 9961136, 9961135, 9961130, 9960967, 9954899,
9954868
```

```
9942162, 9942152, 9912555, 9912538, 9906591, 9906422, 9900343,
9900252
9860271, 9848013, 9843599, 9843521, 9843484, 9838472, 9838425,
9838423
9825943, 9806943, 9787581, 9756071, 9742879, 9722918, 9712493,
9705800
9661026, 9621575, 9609052, 9602442, 9596286, 9596134, 9584318,
9544364
9537886, 9531846, 9497201, 9477563, 9398011, 9386088, 9356910,
9350744
9344456, 9344421, 9338225, 9294503, 9294467, 9270774, 9270705,
9258332
9253152, 9231915, 9219751, 9215275, 9154584, 9154577, 9124550,
9122853
9118620, 9118618, 9106561, 9094364, 9060003, 9032502, 8977749,
8943577
8918857, 8914871, 8904512, 8897154, 8868765, 8849938, 8826372,
8813180
8782751, 8782221, RE44701, 8595819, 8595791, 8595383, 8584199,
8464333
8423676, 8387128, 8332925, 8312507, 8291487, 8266235, 8151322,
8079077
7979585, 7804956, 7716378, 7665138, 7675854, 7647635, 7627672,
7596695
7577833, 7552126, 7392241, 7236491, 7139267, 6748084, 6658114,
6535516
6363075, 6324286, 8392563, 8103770, 7831712, 7606912, 7346695,
7287084
6970933, 6473802, 6374300

64-bit Advanced Core OS (ACOS) version 6.0.1-d, build 145
(Jun-04-2023,08:02)
Booted from Hard Disk primary image
Number of control CPUs is set to 4
Serial Number: TH760D5022440001
Firmware version: 1538.0
aFleX version: 2.0.0
GUI primary image (default) version 6_0_1-d-6_0_1-d-17
GUI secondary image version 5_2_1-P7-5_2_1-P7-23
aXAPI version: 3.0
```

```
Hard Disk primary image (default) version 6.0.1-d, build 145
Hard Disk secondary image version 5.2.1-P7, build 160
Compact Flash primary image (default) version 5.2.1-p3, build
70
Last configuration saved at Jun-23-2023, 18:44
Hardware: 96 CPUs(Stepping 7), Total 464G drive
Total System Memory 193606 Mbytes
Hardware Manufacturing Code: 224411
Hotfixes Applied below: HF-ACOS-16
Current time is Jun-27-2023, 11:09
The system has been up 3 days, 16 hours, 28 minutes
```

show vlans

Description Display the configured VLANs.

Syntax

```
show vlans [vlan-id]
```

Parameter	Description
vlan-id	View information for the specified VLAN only (1-4094).

Mode All

Example The following command lists all the VLANs configured on an ACOS Device:

```
ACOS# show vlans
Total VLANs: 4
VLAN 1, Name [DEFAULT VLAN]:
Untagged Ethernet Ports:    3   4   6   7   8   9  10  11
                           12  13  14  15  16  17  18  19
                           20
  Tagged Ethernet Ports:   None
 Untagged Logical Ports:   None
   Tagged Logical Ports:   None

VLAN 60, Name [None]:
Untagged Ethernet Ports:   None
  Tagged Ethernet Ports:    2
```

```
 Untagged Logical Ports:   None
   Tagged Logical Ports:   None

       Router Interface:   ve 60

VLAN 100, Name [None]:
Untagged Ethernet Ports:   None
  Tagged Ethernet Ports:    5
 Untagged Logical Ports:   None
   Tagged Logical Ports:   None

       Router Interface:   ve 100

VLAN 120, Name [None]:
Untagged Ethernet Ports:   None
  Tagged Ethernet Ports:    1
 Untagged Logical Ports:   None
   Tagged Logical Ports:   None

       Router Interface:   ve 120
```

show vlan counter

Description Show the number of counters on VLAN configured on the ACOS device. All the packets received on shared VLAN in a shared partition are accounted on shared partition interface VE statistics. Packets which are switched from shared partition to L3V partitions are accounted in L3V partition interface VE interface stats. The dropped packets are updated in "**show slb switch**" and "**show system platform statistics**" drop counters. A total number of packets which are switched from shared partition to private partition are accounted and showed under "**show vlan counters**".

Syntax

```
show running-config | sec partition p1
```

```
partition p1 id 1

    shared-vlan
      vlan 202
      allowable-ip-range 80.80.80.0/24
```

```
      allowable-ip-range 90.90.90.0/24
      allowable-ip-range 100.100.100.0/24
      allowable-ip-range 57.57.57.4/32
      allowable-ip-range 57.57.57.25/32
      allowable-ip-range 57.57.57.104/32
      allowable-ipv6-range 1111::/64
      allowable-ipv6-range 3333::/64
{
  "partition": {
    "partition-name":"p1",
    "id":1,
    "uuid":"189bd238-e3d4-11e6-b239-001fa001f020",
    "shared-vlan": {
      "vlan":202,
      "allowable-ip-range": [
        "80.80.80.0/24",
        "90.90.90.0/24",
        "100.100.100.0/24",
        "57.57.57.4/32",
        "57.57.57.25/32",
        "57.57.57.104/32"
      ],
      "allowable-ipv6-range": [
        "1111::/64",
        "3333::/64"
      ],
      "mgmt-floating-ip-address":"57.57.57.4",
      "vrid":1,
      "uuid":"19ad5ee4-e3e3-11e6-b5ba-001fa001f020",
      "a10-url":"/axapi/v3/partition/p1/shared-vlan"
    }
  }
}

AX2500#show running-config | sec vlan 202
vlan 202
  shared-vlan
  tagged ethernet 7
  router-interface ve 202
```

```
AX2500#show json-config vlan 202
a10-url:/axapi/v3/network/vlan/202
{
  "vlan": {
    "vlan-num":202,
    "shared-vlan":1,
    "tagged-eth-list": [
      {
        "tagged-ethernet-start":7,
        "tagged-ethernet-end":7
      }
    ],
    "ve":202,
    "uuid":"1978a41a-e3e3-11e6-b5ba-001fa001f020"
  }
}
```

Mode

show slb switch
show system platform statistics
show vlan counters

Parameter	Description
begin	Begin with the line that matches
include	Include lines that match
exclude	Exclude lines that match
section	Filter a section of output
<2-4094>	Show specific VLAN counters
name	Name of the counter
Broadcast counter	The number of broadcast counters
Multicast counter	The number of multi-cast counter
IP Multicast counter	The number of IP multi-cast counter
Unknown Unicast counter	The number of unknown uni-cast counter
Mac Movement counter	The number of Mac movement counter

Parameter	Description
SVLAN Partition switched counter	The number of SVLAN partition switched counter
vlan-num	The number of VLANs
detail	Print per CPU stats
ethernet	Specification regarding ethernet port
cpu-load-sharing	Displaying information about CPU load sharing

Usage To use this command, you must be logged in with an admin account that has root, Global read, or Global write privileges.

Example The following command shows that the **vlan counter** currently being managed in this configuration, by the CLI session in the shared partition:

```
AX2600#show vlan counter 202
-------------------------------------------------------
Counter                                          Value
-------------------------------------------------------
Broadcast counter                                    0
Multicast counter                                    1
IP Multicast counter                                 0
Unknown Unicast counter                              0
Mac Movement counter                                 0
SVLAN Partition switched counter                   268
vlan-num                                           202
```

show vlan counters

Description View statistics/counters for configured VLANs or a specific VLAN.

Syntax **show vlan counters** [*vlan-id*]

Parameter	Description
vlan-id	View counters for the specified VLAN only (2-4094).

Mode All

Example Example output for this command, for a specific VLAN:

```
ACOS> show vlan counters 10
Broadcast counter                                    1
Multicast counter                                    14
IP Multicast counter                                 0
Unknown Unicast counter                              0
Mac Movement counter                                 0
```

show vpn

Description Show VPN information.

Syntax

```
show vpn [
  all-partitions |
  crl |
  default |
  ike-sa |
  ike-stats |
  ike-stats-global |
  ipsec-sa |
  log |
  ocsp
  partition {shared | partition-name}
]
```

Parameter	Description
all-partitions	Show VPN configuration summary for all partitions.
crl	Show cached VPN Certificate Revocation Lists (CRL) certificates.
default	Show default VPN configuration.
ike-sa	Show VPN IKE Security Association (SA).
ike-stats	Show VPN IKE statistics.
ike-stats-global	Show VPN IKE global statistics.
ipsec-sa	Show VPN IPsec Security Association (SA).
log	Show VPJN log and debug information.
ocsp	Show cached VPN Online Certificate Status

Parameter	Description
	Protocol (OCSP) certificates.
partition	Show VPN configuration for the specified partition only.

Mode All

Example Below is an example output for this command.

```
ACOS# show vpn
IKE Gateway total:    0
IPsec total:          0

IKE SA total:         0
IPsec SA total:       0

IPsec mode: software
IPsec passthrough traffic

CPU 0 processed 0 packets
```

clear dns cache

Description Clears DNS caching information.

Syntax

```
clear dns cache [ entry options | global options | statistics
| template <template-name> options | virtual-server <virtual_
server_name> <virtual_port> <port_type> options ]
```

Parameter	Description
entry *options*	Clears DNS cache entries from the system-wide cache. Filters can be applied.

Parameter	Description
global *options*	Clears global DNS cache entries. Filters can be applied.
statistics	Clears DNS caching statistics.
template *<template_name> options*	Clears DNS entries from the shared cache of the specified DNS template. Filters can be applied.
virtual-server *<virtual_server_name> <virtual_port> <port_type> options*	Clears DNS cache entries for the specified virtual server, vPort, and port type. Filters can be applied.

The following *options* are available for filtering DNS cache entries:

Parameter	Description
dns-class *suboptions*	Clears entries matching the specified DNS class. The following *suboptions* are available: • **IN** – INTERNET class • **CH** – CHAOS class • **HS** – HESIOD class • **NONE** – NONE class • **ANY** – ANY class • *num* – Custom class value (1-65535)
dns-type *suboptions*	Clears

Parameter	Description
	entries matching the specified DNS cache record type. The following *suboptions* are available: • **A** – Address type • **AAAA** – IPv6 Address type • **CNAME** – Canonical name type • **MX** – Mail exchange type • **NS** – Name server type • **SRV** – Service locator

Parameter	Description
	• **PTR** – PTR resource type • **SOA** – Start of authority type • **TXT** – Text type • **ANY** – All cached type • *num* – Custom type value (1-65535)
domain *suboptions*	Clears DNS cache entries for a specific domain. The following *suboptions* are available: • **dns-domain-name** – Domain name

Parameter	Description
	• **fqdn-domain** – Fully qualified domain name

Mode Privileged EXEC mode or global configuration mode.

Usage Use this command to clear DNS cache entries system-wide, per DNS template, or per virtual server/port. The supported filters may be used individually or in combination (multiple-choice filtering).

- You can remove all entries or selectively clear them using filters.
- You can clear DNS statistics counters.

NOTE: If the specified virtual server, virtual port, or DNS template does not exist, the system returns no output.

Limitation The clearing of shared cache entries from other L3V partitions is not supported.

Example The following command clears DNS caching statistics:

```
ACOS(config)# clear dns cache statistics
```

Example The following command clears the global DNS cache based on the domain name:

```
ACOS(config)# clear dns cache global domain-name dns-domain-name foo.com
```

Example The following command clears DNS cache entries of type CNAME:

```
ACOS(config)# clear dns cache entry dns-type CNAME
```

Example The following command clears the DNS cache entries for DNS class 55:

```
ACOS(config)# clear dns cache entry dns-class 55
```

Example The following command clears entries from the shared cache of a DNS template using a domain filter:

```
ACOS(config)# clear dns cache template dns_template domain-name dns-domain-name test.example.com
```

Example The following command clears DNS cache entries for a specific virtual server, vPort, and port type using a DNS type filter:

```
ACOS(config)# clear dns cache virtual-server vs3 53 dns-udp dns-type CNAME
```

clear ip dns cache

Description Clear or refresh the DNS cache of virtual partitions.

Syntax

```
clear ip dns-cache
```

Default NA

Mode All

```
ACOS# clear ip dns-cache
ACOS# clear counters service-ip serviceip1
ACOS# clear counters zone dns-zone-name
```

clear system table-integrity

Description Manually sync all the ARP, ND6, MAC, IPv4 FIB, and IPv6 FIB tables between the processing units.

NOTE:

- The command is applicable only to FTA-devices.
- There should be a 30 seconds gap between consecutive manual-sync command `clear system table-integrity [all | arp | ipv4-fib |ipv6-fib | mac | nd6]`.

Syntax

```
For Shared partition - clear system table-integrity [all | arp | ipv4-fib | ipv6-fib | mac | nd6]
```

```
For L3V partition - clear system table-integrity [all | ipv4-
fib | ipv6-fib]
```

Parameter	Description
arp | ipv4-fib | ipv6-fib | mac | nd6	Sync ARP/MAC/ND6 tables across all the partitions. IPv4/IPv6 FIB will only be synced for the shared partition.
ipv4-fib | ipv6-fib	Sync IPv4/ IPv6 FIB tables in the L3V partition.

Syntax

```
Clear command for statistics:
clear system table-integrity [all | arp | ipv4-fib |ipv6-fib |
mac | nd6] statistics
```

Mode Privileged EXEC mode or global configuration mode

Application Delivery Partition

An Application Delivery Partition (ADP) is a partition that is added to the device. An administrator account with root access has read-write privileges to all ACOS objects across all partitions. ADPs are also referred to as *Private Partitions*. ACOS is initially provisioned with one partition (named shared) and provisioned with one administrator account (named admin). Additional partitions and administrator accounts can be added to the device through CLI and GUI commands.

NOTE: Configuring administrator accounts is described in *Management Access and Security Guide*.

This reference lists the CLI configuration and show commands that apply specifically to ADP.

Configuration Commands

active-partition

Description Switch to a different Application Delivery Partition (ADP) on your ACOS Device.

Syntax

```
active-partition {partition-name | shared}
```

Parameter	Description
partition-name	Name of the L3V partition you want to switch to.
shared	The shared partition.

Mode Available at any CLI level.

Usage Root admins or admins with Global read or Global write privileges can select the partition to view. When an admin with one of these

privilege levels logs in, the view is set to the shared partition by default, which means all resources are visible.

Example The following command changes the view to L3V partition "**companyA**":

```
ACOS# active-partition companyA
Currently active partition: companyA
ACOS[companyA]#
```

The name of the partition is shown in the CLI prompt.

application-type

Description Configure the **shared** partition for either SLB or CGN applications.

Syntax

```
[no] application-type {adc | cgnv6}
```

Default All CLI commands for the prompt level are accessible until either the **adc** or **cgnv6** option is specified. After that, commands from the other are no longer available.

Mode Global configuration mode.

partition

Description Configure a L3V partition.

Syntax

```
[no] partition partition-name id num
[application-type {adc | cgnv6}]
```

Parameter	Description
partition-name	Specifies the name of the L3V partition.
id *num*	Assigns an ID to the partition. The partition ID ensures that a partition's configuration remains consistent across devices in multi-device deployments (for example, VRRP-A or aVCS).

Parameter	Description
application-type {**adc** | **cgnv6**}	Specifies whether this L3V partition will be used to configure SLB or CGN applications. Once one is specified, commands and options from the other are no longer accessible in the partition. You can change the application type at any time as long as you have not configured the partition specifically for SLB or CGN. Once you do, you must remove all such configuration before being allowed to change the application type.

This command changes the CLI to a sub-command mode, where the following commands are available:

Command	Description
shared-vlan	Configure a shared VLAN in the partition. The shared-vlan command inside a partition places the user in a new mode.
template	Attach a resource accounting template to this partition. Resource accounting templates are created using the system resource-accounting template command.

Default The ACOS Device has a shared partition but no L3V partitions by default.

Mode Global configuration mode

Usage To use this command, you must be logged in with an admin account that has Global write privileges.

If you delete a partition, resources associated with the partition are permanently deleted. This includes SSL certificates and keys, and aFleX scripts. These resources are deleted even if you reload or reboot without saving the configuration. In this case, the partition configuration is restored but the resources are still gone.

Example The following commands configure two partitions, “companyA” (used for SLB configuration) and “companyB” (used for CGN configuration):

```
ACOS(config)# partition companyA id 1 application-type adc
ACOS(config-partition:companyA)# exit
ACOS(config)# partition companyB id 2 application-type cgnv6
ACOS(config-partition:companyB)#
```

To change the “companyB” partition so that it can be used for SLB configuration, issue the same command and replace **cgnv6** with **adc**:

```
ACOS(config)# partition companyB id 2 application-type adc
ACOS(config-partition:companyB)#
```

This is valid as long as you do not make any SLB-specific or CGN-specific configuration inside the partition. Once you do, you must remove all such configuration before you will be allowed to change the application type of the partition.

Example The following command removes the partition “companyA”:

```
ACOS(config)# no partition companyA id 1
Remove this partition and keep configurations on the disk?
(y/n) y
ACOS(config)# delete partition companyA id 1
The operation will delete this partition permanently from all
profiles on disk.
This action is not recoverable. Continue? [yes/no]: yes
```

The **no partition** command unloads the partition but keeps the configuration on your system. To perform a hard delete of the partition and associated configuration, you must also use the **delete partition** command.

partition-admin

Description Configure an admin account in the L3V partition. The created partition admin user is valid even if the creator admin user is removed.

The current L3V partition is assigned automatically to the user, another partition cannot be specified. To see all the admin users assigned to an L3V partition, use the `show admin` command.

NOTE: This command does not support Service Partitions. Remote users such as Radius and LDAP are also not supported.

Syntax

```
[no] partition-admin partition-admin-username
```

This command changes the CLI to the configuration level for the specified admin account, where the following admin-related commands are available:

Command	Description
`access { axapi | cli | web }`	Configure the access type, i.e., specify the user interfaces through which the partition admin can access the partition. The following options are available: • `axapi` - Allow access through aXAPI. • `cli` - Allow access through ommand line interface. • `web` - Allow access through Web GUI. By default, access is allowed through all user interfaces (CLI, GUI, and aXAPI).
`disable`	Disables the partition admin user account. By default, the partition admin user accounts are enabled when they are added.
`enable`	Enables the partition admin user account. By default, the partition admin user accounts are enabled when they are added.
`password` *`string`*	Configures the password for the user account. Specify the password string (1-63 characters). The character range is platform-specific. Passwords

Command	Description
	are case sensitive and can contain special characters. (For more information, see Adding Special Character in Strings.)
`privilege` *`level`*	Configures the privileges for the user account. The following options are available: • `partition-read` – The user has read-only privileges within the L3V partition. • `partition-write` – The user has read-write privileges within the L3V partition. • `partition-enable-disable` – The user has read-only privileges for real servers, with permission to view service port statistics and to disable or re-enable the servers and their service ports. No other read-only or read-write privileges are granted. **NOTE:** Health monitor (HM) privilege is not supported. For more information, see For more information, see *Configuring Application Delivery Partitions* guide. The default privilege is `partition-read`.
trusted-host { *`ipaddr/mask-length`* | *`ipaddr subnet-mask`* }	Specifies the subnet address from which the partition-admin user will be allowed access to the ACOS device. You can specify a specific subnet (mask or length). The default trusted host is 0.0.0.0/0, which allows access from any host or subnet.

Default The default partition admin user account has `partition-read` privileges.

Mode Configuration mode

Usage The following points need to be considered while creating a partition admin account:

- Only admins with `write` and `partition-write` privileges can create accounts.
- A partition admin user cannot modify L3V users created using the **`admin`** command.
- A partition admin user cannot create another user with same name as the system admin or a user in other partition.
- After logging into a partition-admin account, executing the `show admin` command displays only the users of that partition. For example, if you log in as *`p3-user`* (under partition *`p3`*), you will only see the users of partition *`p3`*.

NOTE: The **`admin`** command can only perform the following actions on partition-admin users: **`disable/enable`**, **`delete`**, and **`lock/unlock`**. For any other changes, the system administrator needs to switch to the corresponding partition and make modifications.

Example The following commands create a partition admin *`user1`* with password *`1234`* in the partition *`Partition_1234`*:

```
ACOS[Partition_1234](config)# partition-admin user1
ACOS[Partition_1234](config-partition-admin:user1)# password
1234
ACOS[Partition_1234](config-partition-admin:user1)# show admin
Total number of configured users: 2
Privilege R: read-only, W: write, P: partition, HM: external
health monitor, En: Enable
Access Type   C: cli, W: web, A: axapi
UserName Status Privilege Access UserType Partition
------------------------------------------------------------
------
admin Enabled   R/W/HM    C/W/A  Local
user1 Enabled   P.R       C/W/A  Local    Partition_1234
```

Example The following command changes the privilege of the partition admin user from `partition-read` (default) to `partition-write`:

```
ACOS[Partition_1234](config-partition-admin:user1)# privilege
partition-write
Modify Admin User successful!
ACOS[Partition_1234](config-partition-admin:user1)# show admin
Total number of configured users: 2
Privilege R: read-only, W: write, P: partition, HM: external
health monitor, En: Enable
Access Type   C: cli, W: web, A: axapi

UserName Status Privilege Access UserType Partition
------------------------------------------------------------
------
admin Enabled   R/W/HM   C/W/A   Local
user1 Enabled   P.R/W    C/W/A   Local    Partition_1234
```

Example The following command deletes a partition admin user. The partition admin user cannot be deleted without logging off.

```
ACOS[Partition_1234](config-admin:user1)# exit
ACOS[Partition_1234](config)# no partition-admin user1
```

partition-group

Description Create a named set of partitions.

Syntax

```
[no] partition-groupgroup-name
```

Replace *group-name* with the name of the group for the set of partitions.

This command changes the CLI to the configuration level for the group, where the following command is available.

Parameter	Description
member *partition-name*	Adds a partition to the group. You can specify one partition name on the command line. To add additional partitions re-enter the command for each partition.

Default None.

Mode Global configuration mode

Example The following example creates a group called “slbgroup” and adds the L3V partition “companyA” as a member:

```
ACOS(config)# partition-group slbgroup
ACOS(config-config-partition-group:slbgroup)# member companyA
```

Usage When partitions are grouped to form a partition group, CGN NAT pool can be shared with a partition or a partition group. All the members of the specified partition group share the common CGN pool resources.

service-partition

Description Configure a service partition. A service partition is created from the shared partition.

When a partition is deleted, resources associated with the partition are deleted, including SSL certificates and keys, and aFleX scripts. These resources are deleted if the device is reloaded or rebooted without saving the configuration. In this case, the partition configuration is restored but the resources are still gone.

Syntax

```
[no] service-partition partition-name id num
application-type adc
```

Parameter	Description
partition-name	Specifies the name of the service partition.
id *num*	Assigns an ID to the partition. The partition ID ensures that a partition’s configuration is consistent across devices in multi-device deployments (for example, VRRP-A or aVCS). Service partitions and L3V partitions use the same pool of ID numbers.
application-type adc	Specifies that the partition is used for SLB applications.

This command changes the CLI to a sub-command mode, where the following command is available:

Command	Description
follow-vrid <*vrid-num*>	Joins the VRRP-A group specified by the VRID number. Valid options for vrid-num ranges from 0 to 7. VRRP commands are not supported within a service partition. Joining the group provides partition access to the VRRP-A group access.

Default The ACOS Device has a shared partition but no service partitions by default.

Mode Global configuration mode

Usage To use this command, you must be logged into the shared partition with an admin account that has write privileges for the parent partition.

Example The following commands configure two partitions from the shared partition: "**companyA**" (L3V) and "**companyB**" (service):

```
ACOS(config)# partition companyA id 1 application-type adc
ACOS(config-partition:companyA)# exit
ACOS(config)# service-partition companyB id 3 application-type
adc
ACOS(config-service-partition:companyB)# exit
ACOS(config)#
```

This command displays the partitions.

```
ACOS[companyA](config)# active-partition shared
Current active partition: shared
ACOS(config)# show partition
Total Number of active partitions : 3
Partition Name    Id      L3V/SP      Parent L3V            App
Type    Admin Count
-------------------------------------------------------------
-------
companyA          1        L3V        -                     ADC
      0
```

```
companyB          3        SP         shared                ADC
      0
ACOS(config)#
```

Example The following command removes the partition "**departmentAA**":

```
ACOS(config)# no service-partition companyB id 3 application-
type adc
Remove this partition and keep configurations on the disk?
(y/n) y
ACOS(config)# delete service-partition companyB id 3
The operation will delete this partition permanently from all
profiles on disk.
This action is not recoverable. Continue? [yes/no]: yes
ACOS(config)#
```

The **no service-partition** command unloads the partition but keeps its configuration on your system. To perform a hard delete of the partition and associated configuration, use the **delete service-partition** command. A service partition can only be unloaded and deleted from the shared partition.

shared-vlan

Description Enable the shared VLAN functionality for the partition.
vlan 100: This is an extended feature of the existing model. It enables the shared VLAN 100 functionality for the partition.

Syntax

```
[no] shared-vlan
```

This command changes the CLI to the shared VLAN configuration level for the partition, where the following parameters are available.

The command **shared-vlan** enables the shared VLAN functionality for **vlan 100**. The command **shared-vlan** under partition p1 places the user in a new mode. The available options in this mode are **vlan**, **allowable-ip-range**, and **mgmt-floating-ip-address**.

```
[no] vlan 100
```

The command **vlan 100** enables the shared VLAN functionality for **vlan 100**.

The command **vlan 100** in **shared-vlan** mode enables the **vlan 100** for shared VLAN feature.

This command changes the CLI to the shared VLAN configuration level for the partition, by enabling the shared VLAN 100 functionality, wherein the following parameters are available.

Parameter	Description
vlan *vlan_id*	VLAN ID to use for the Shared VLAN feature. This VLAN must be configured as a shared VLAN ahead of time.
allowable-ip-range *ip*	IPv4 addresses in this range are used for configuring VE interfaces in partitions and for `mgmt-floating-ip address` configurations. The command **allowable-ip-range** 1.3.4.0/24 assigns 1.3.4.0/24 subnet for partition p1 for shared VLAN feature. Users can configure interface VE 100 and assign IP address with in the subnet 1.3.4.0/24. Users can also configure VIP and NAT pools in partition P1 with in the subnet range for **shared-vlan** feature. Any VIP address configured in partition P1 inside the range of 1.3.4.0/24 cannot be configured with **vr-id** in its partition, because partitions using shared partition feature always use the **vr-id** follow feature in the partition.
allowable-ipv6-range *ip*	The command **allowable-ipv6-range** 1111::0/64 assigns 1111::0/64 subnet for partition p1 for shared VLAN feature. Users can configure interface VE100 and assign IP address with in the subnet 1111::0/64.

Parameter	Description
	User can configure VIP and NAT pools in partition P1 within the subnet range for **shared-vlan** feature. Any VIP address configured in partition P1 inside the range of 1111::0/64 cannot be configured with **vr-id** in its partition, because partitions using shared partition feature always use the **vr-id** follow feature in the partition.
mgmt-floating-ip-address *ip* **vrid** *vrid_id*	This command and the IPv4 address are used for device management in VCS scenarios. In VCS scenarios, all the devices are configured with the same `mgmt-floating-ip-address`. The vMaster owns this IP address and is used to configure all the devices. `The vrid` given with this configuration must also be used in `affinity-vrrp-a-vrid vrid`. It is preferred to use the configuration system `ve-mac-scheme system-mac`, while configuring the shared VLAN feature. The configuration `system ve-mac-scheme system-mac` uses the Mac based lookup to identify the L3V Partition id and this lookup is much faster. The configuration `system ve-mac-scheme system-mac` is not supported in all platforms. In such cases the destination IP address of the packet is used for lookup to identify the L3V Partition id. This feature must work seamlessly in both the cases.

Default Disabled

Mode Shared VLAN

Example

The following example shows configuring the `allowable-ip-range` of 1.3.4.0/24 in partition p1 for the shared VLAN feature.

```
ACOS(config)# partition p1 id 2
ACOS(config-partition:p1)# shared-vlan
ACOS(config-partition:p1-shared-vlan)# allowable-ip-range
1.3.4.0/24
```

The following example shows configuring the allowable-ip-range of 1.3.4.0/24 and 2.3.4.0/24 along with allowable-ipv6-range in partition p1 for the shared VLAN feature, user in a new mode.

```
ACOS(config)# partition p1 id 2
ACOS(config-partition:p1)# shared-vlan
ACOS(config-partition:p1)# shared-vlan vlan-100
ACOS(config-partition:p1-shared-vlan-vlan-100)

# allowable-ip-range 1.3.4.0/24
# allowable-ip-range 2.3.4.0/24
# allowable-ipv6-range 1234::0/64

vlan 100
untagged ethernet1
shared-vlan
router-interface ve 100

vlan 200
untagged ethernet2
shared-vlan
router-interface ve 200

interface ve 100
ip address 80.1.1.1/24
ipv6 address 1111::3/64

interface ve 200
ip address 90.1.1.1/24
ipv6 address 9000::1/64

vcs device 1
affinity-vrrp-a-vrid 10
```

```
partition one id 10
shared-vlan
vlan 100

mgmt.-floating-ip-address 80.1.1.10 vr-id 10
allowable-ip-range 80.1.1.0/24
allowable-ip-range 99.1.1.96/27
allowable-ipv6-range 1111::/64
allowable-ipv6-range 2222::/64
```

From the above configuration, there are two ipv4 address and one ipv6 address ranges assigned to the partition one.

```
- 80.1.1.0/24
- 99.1.1.96/27
- 1111::/64
- 2222::/64
```

As an example, the first subnet is matching the interface VE 100 IPv4 address configuration in shared partitions.

The user can pick IP address in these ranges for the VIPs and management address.

If the user picks the 80.1.1.4 for management purpose, then the configuration for this IP address on interface VE 100 can only be done within private partition one. The second subnet is not matching any interface IPv4 address configuration subnet.

This range must only be used for VIP configurations. The user can pick any IP address in the first subnet range to configure VIP.

NOTE: The configuration for `mgmt.-floating-ip-address` is optional. It is used in scenarios where the user wants to have a single management address to configure both VRRP active and standby nodes in VCS environments. `ssh` to this address lands in specific partition of the active device in the group-id. The command `mgmt-floating-ip-address` is only applicable for IPv4 and it is not supported for IPv6. The user is free to pick any prefixes from 1111::/64 and 2222::/64 for his IPv6 VIP configuration. There is no support for management services in shared VLAN for IPv6. The user cannot assign IPv6 address in partition one for interface VE100.

```
Add partition configuration

one]#show running-config
Interface ve 100
Ip address 80.1.1.4 /24

Interface ve 200
Ip address 90.1.1.4 /24

ip nat pool pool1 80.1.1.2 80.1.1.3 netmask /32

ipv6 nat pool v6nat 5555::25 5555::25 netmask 64 vrid 1

slb virtual-server vip 99.1.1.96
port 5000 tcp

slb virtual-server vs1 1111::25
port 80 tcp
```

Usage In this example, any VIP address configured in partition P1 within the range 1.3.4.0/24 cannot be configured with a `vrid` in its partition because partitions using the shared VLAN will always use the `vridfollow` feature in the partition.

Show Commands

show active-partition

Description Show the active partition currently being managed by the CLI.

Syntax

```
show active-partition
```

Mode All

Example The following command shows that the partition currently being managed by the CLI session is the shared partition:

```
ACOS# show active-partition
Currently active partition: shared
```

show partition

Description Show the private (L3V and service) partitions configured on the ACOS Device

Syntax

```
show partition [all | available-id | port-ownership]
```

Parameter	Description
all	View all partitions on the device, both active and inactive. Without this option, only active partitions are displayed.
available-id	View the IDs available for partition creation. Since partition ID mapping remains with a partition for the partition lifetime, this option is useful to view which IDs aren't available on the system for the creation of a new partition.
port-ownership	View the port ownership information for each partition on the device. The output provides information about which ports are in use by which partitions.

Mode All

Usage To use this command, you must be logged in with an admin account that has root, Global read, or Global write privileges.

Example The following command all active partitions configured on an ACOS Device:

```
ACOS# show partition
Total Number of active partitions: 3
Partition Name    Id    L3V/SP   Parent L3V   App Type    Admin
Count
-------------------------------------------------------------
-------
LV-1              2     L3V      -            ADC         0
SR-1              3     SP       shared       ADC         1
SR-9              9     SP       shared       ADC         0
```

The following table describes the fields in the command output.

Field	Description
Total Number of active partitions	Number of partitions configured and being used on the system.
Partition Name	Name of the L3V partition.
Id	ID of the L3V partition.
L3V/SP	Indicates the ADP type: L3V or Service.
Parent L3V	Specifies the partition under which the partition was created. In this version, the parent of all service partitions is the shared partition. This field is irrelevant for L3V partitions.
Admin Count	Number of admins configured for the partition.

show partition-config

Description View the running-config for all partitions, or a specific L3V partition on the system.

This command replaces the **show configuration** command from previous releases.

Syntax

```
show partition-config {all | shared | name}
```

Parameter	Description
all	View the running-config for all partitions on the system. This is the default option if no specific partition is specified. aflex-scripts - This parameter is also available for viewing aFleX scripts along with the partitions.
shared	View the running-config for the shared partition only.
name	View the running-config for the specified L3V partition only.

Mode All

Example The example below shows how to view the running-config for partition “companyB” (truncated for brevity):

```
ACOS# show partition-config companyB
!Current configuration: 1605 bytes
!Configuration last updated at 12:16:37 IST Tue Sep 30 2014
!Configuration last saved at 11:34:33 IST Tue Sep 30 2014
!
active-partition companyB
!
ip access-list test
        remark 123
!
!
ipv6 access-list test
        remark 123
!
```

```
!
...
```

show partition-group

Description Show configured L3V partition groups.

Syntax

```
show partition-group
```

Parameter	Description
name	Show the group members for a specified group name.

Mode All

Example Below is an example output for this command:

```
ACOS# show partition-group
partition-group slbgroup
 member companyB
 member companyA
!
ACOS#
```

ACOS Virtual Chassis System

ACOS Virtual Chassis System (aVCS) enables you to manage a cluster of ACOS devices like a single, virtual chassis. One ACOS device in the virtual chassis is the virtual master (vMaster). The other ACOS devices are virtual blades (vBlades) within the virtual virtual chassis, and are managed by the vMaster. As a controller for the vBlades, the vMaster provides centralized storage of the entire ACOS device configuration. Any configuration changes from the vMaster are automatically propagated to the vBlades.

aVCS, as a management tool, provides high availability functionality on the ACOS device with the help of VRRP-A across multiple ACOS devices.

This reference lists the CLI configuration and show commands that apply specifically to aVCS.

Configuration Commands

device-context

Description Changes the context of the CLI session from the vMaster to a vBlade, in order to configure the vBlade.

This command is used to configure device-specific and routing settings for an ACOS Device in an aVCS environment. To configure an aVCS-related settings for a device in an aVCS environment, use the vcs device command.

This command can also be applied to certain non-routing configuration commands (for example, LACP).

NOTE: This command replaces the **`router device-context`** command in previous releases.

Syntax

```
device-context DeviceID
```

Replace *DeviceID* with the ID of the target device. The target device is the device you plan to access. The acceptable values for this parameter will vary depending on your specific hardware platform.

Default By default, the vMaster for the virtual chassis is the context of the management session.

Mode Configuration mode

Example The following command changes the configuration context to device 3 in a virtual chassis, and changes the hostname of that device to "ACOS3:"

```
ACOS(config)# device-context 3
All the following configuration will go to device 3
ACOS(config)# hostname ACOS3
ACOS3(config)#
```

vcs admin-session-connect

Description Opens an SSH admin session with a device in an aVCS.

Syntax

```
vcs admin-session-connect device DeviceID
```

Replace *DeviceID* with the ID of the target device. The target device is the device you plan to access. The acceptable values for this parameter will vary depending on your specific hardware platform.

Default By default, the CLI session is on the device you logged onto.

Mode Global Config (on vMaster only)

Usage This command does not apply to device-specific configuration commands. To enter device-specific configuration commands on another device, use the device-context command instead.

Entering this command on the vMaster creates an SSH connection to the vBlade, without a password prompt. After the connection is established, you can enter configuration commands to take effect on the vBlade.

While the connection to the vBlade is in effect, configuration commands cannot be entered directly on the vBlade through any other management connections.

If an SSH security warning about the RSA fingerprint is displayed:

- If the RSA fingerprint is correct, enter **yes**.
- If the RSA fingerprint does not match, enter **no**. Someone may be attempting to spoof the device in order to gain information about the system or network access.

Example

The following command changes the CLI session to aVCS device 2. In this example, this is the first time the command has been used to access device 2.

```
ACOS-device1(config)# vcs admin-session-connect device 2
spawn ssh -l admin 192.168.100.126
The authenticity of host '192.168.100.126 (192.168.100.126)'
can't be established.
RSA key fingerprint is
ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.126' (RSA) to the list
of known hosts.
Last login: Thu Feb 23 03:33:37 2017 from 10.254.101.80

ACOS system is ready now.

[type ? for help]

TIS-Standby-vBlade[1/2]>enable
Password:***
Last login: Thu Jul 22 21:06:46 2010 from 192.168.3.77
ACOS-device2#
```

At the Password prompt, enter the password for the admin account on the target device.

Example

The following example shows the CLI response if you accidentally try to switch to the device you are already on:

```
ACOS-device1(config)# vcs admin-session-connect device 1
```

```
Unnecessary to do such operation to manage local device
```

vcs database-distribution

Description Enables or disables the database cluster distribution.

Syntax

```
vcs database-distribution {enable | disable}
```

Parameter	Description
enable	Enables database cluster distribution.
disable	Disables database cluster distribution.

Default Disabled

Mode Configuration mode

Usage This command enables the aVCS for Scaleout.

Example The following command enables the aVCS for Scaleout:

```
ACOS-Active-vMaster[1/1](config)# vcs database-distribution
enable
ACOS-Active-vMaster[1/1](config)#
```

vcs disable

Description Disables aVCS on the device.

Syntax

```
vcs disable
```

Default N/A. This is an operational command rather than a configuration command.

Mode Privileged EXEC (vMaster or vBlade)

Usage In addition to disabling aVCS on the current device, you can also use device-context to disable aVCS on another device.

Example The following command disables aVCS on the current device:

```
ACOS-Active-vMaster[1/1]# vcs disable
```

```
ACOS-Active-vMaster[1/1]#
```

Example The following commands switch to device 2 from device 1, then disables aVCS on device 2:

```
ACOS-Active-vMaster[1/1]# configure
ACOS-Active-vMaster[1/1](config:1)# device-context 2
All the following configuration will go to device 2
ACOS-Active-vMaster[1/1](config:2)# vcs disable
ACOS-Active-vMaster[1/1](config:2)#
```

vcs enable

Description Enablea aVCS on the device.

Syntax

```
vcs enable
```

Default N/A. This is an operational command rather than a configuration command.

Mode Privileged EXEC (vMaster or vBlade)

Usage After you enter the **vcs enable** command, you must enter the **vcs reload** command to place any aVCS configuration changes into effect and activate the feature.

Before using this command, many of the aVCS commands are not available from the CLI.

The following example shows the commands available prior to running the **vcs enable** command:

```
ACOS(config)# vcs ?
  failure-retry-count  VCS retry count after fails to join the
chassis
  vMaster-maintenance  During this period, vMaster can leave
and come back to
                       be vMaster again
  enable               enable VCS
  disable              disable VCS
ACOS(config)# vcs
```

In addition to enabling aVCS on the current device, you can also use device-context to enable aVCS on another device.

Example The following example enables aVCS on the current device:

```
ACOS-Active-vMaster[1/1]# vcs enable
ACOS-Active-vMaster[1/1]#
```

Example The following example switches to device 2 from device 1, then enables aVCS on device 2:

```
ACOS-Active-vMaster[1/1]# configure
ACOS-Active-vMaster[1/1](config:1)# device-context 2
All the following configuration will go to device 2
ACOS-Active-vMaster[1/1](config:2)# vcs enable
ACOS-Active-vMaster[1/1](config:2)#
```

vcs dead-interval

Description Configures the number of seconds the vBlade devices waits for a keepalive message from the vMaster, before assuming the vMaster is unavailable and triggering vMaster re-election.

Syntax

```
[no] vcs dead-interval seconds
```

Replace *seconds* with the maximum number of seconds to wait for a keepalive message from the vMaster before triggering vMaster re-election. You can specify 0-240 seconds.

Default 10

Mode Global Config (vMaster only)

Example The following command sets the interval to 20 seconds:

```
ACOS-Active-vMaster[1/1](config:1)# vcs dead-interval 20
```

vcs dead-interval-mseconds

Description Configures the number of milliseconds the vBlade devices waits to receive the keepalive message from the vMaster, before assuming the

vMaster is unavailable and triggering vMaster re-election.

Syntax

```
[no] vcs dead-interval-mseconds milliseconds
```

Replace *milliseconds* with the maximum number of milliseconds to wait for a keepalive message from the vMaster before triggering vMaster re-election. You can specify 100-900 milliseconds.

Default 0

Mode Global Config (vMaster only)

Example The following command sets the interval to 320 milliseconds:

```
ACOS-Active-vMaster[1/1](config:1)# vcs dead-interval-mseconds
320
```

NOTE: For the `vcs dead-interval-mseconds` and the `vcs time-interval-mseconds` commands to work, you must configure in the following order:

```
vcs time-interval-mseconds 200
vcs dead-interval-mseconds 900
vcs time-interval 0
vcs dead-interval 0
```

vcs debug

Description Enables aVCS debugging.

Syntax

```
[no] vcs debug {daemon | election | info | vblade | vmaster}
```

Parameter	Description
daemon	Enables debugging for the aVCS process.
election	Enables debugging for vMaster election.
info	Enables display of informational messages in the debugging output.
vblade	Enables debugging for vBlade-related operations.
vmaster	Enables debugging for vMaster-related operations.

Default Disabled

Mode Privileged EXEC (on vBlade); Privileged EXEC and Global Config (on vMaster)

Example The following commands enable debugging for aVCS vMaster operations and display the output:

```
ACOS-Active-vMaster[1/1](config:1)# vcs debug vmaster
ACOS-Active-vMaster[1/1](config:1)# show vcs debug
Debugging switches:                             vmaster,
Debugging Buffer Size:                          8 MB
2010/08/02 10:46:02, [vMaster], vBlade 0, msg loop, received
msg 21
2010/08/02 10:46:02, [vMaster], vBlade 0, msg loop, sent msg
20
...
```

vcs device

Description Adds a device to an existing aVCS, and configure aVCS-related settings for the specified device.

To configure device-specific or routing settings for an ACOS Device in an aVCS environment, use the device-context command.

Syntax

```
[no] vcs device device-id
```

Replace *device-id* with the device ID. The acceptable values for this parameter will vary depending on your specific hardware platform.

This command changes the CLI to the configuration level for the specified aVCS device, where the following aVCS-related commands are available.

Command	Description
[no] affinity-vrrp-a-vrid	Configures a vMaster failover to the Active device on a specified VRID (device running VRRP-A). Use this command on each device that is part of the aVCS

Command	Description
vrid-group	cluster, including the Active device.
[no] **enable**	Enables aVCS on the device. aVCS is disabled by default.
[**no**] **interfaces** {**ethernet** *portnum* | **management** | **trunk** *trunk-num* | **ve** *ve-num*}	Device interfaces used for aVCS vMaster election traffic. You can specify up to 6 election interfaces. For vMaster election to work, the other devices in the virtual Multi-PU platform must be able to reach the device on the specified interface(s).
[**no**] **priority** *num*	Priority of this device for vMaster election, 1-255. Higher priority values are preferred over lower ones. The default priority is 0 (not set).
[**no**] **unicast-port** *portnum*	Protocol port used to create TCP connection between the vMaster and vBlade. This connection is used for configuration synchronization. The range is 1024-65535. The default unicast port is 41216.

Default No aVCS devices are configured by default. When you add an aVCS device, its parameters have the default values described in the table above.

Mode Global Config (vMaster only)

Usage The election interfaces for devices in an aVCS virtual chassis platform must be in the shared partition. Use of an L3V private partition's interface as an aVCS election interface is not supported.

Example The following commands add device 3 to an existing aVCS Multi-PU platform. The management interface will be used for aVCS election traffic and its priority is 3.

```
ACOS-Active-vMaster[1/1](config:1)# vcs device 3
```

```
ACOS-Active-vMaster[1/1](config:1-device:3)# interfaces
management
ACOS-Active-vMaster[1/1](config:1-device:3)# priority 3
ACOS-Active-vMaster[1/1](config:1-device:3)# enable
```

vcs discovery-mode

Description Supports L3 communication in Scaleout.

Syntax

```
[no] vcs discovery-mode ?
```

Replace ? with Unicast, Mcast, or Mixed.

Parameter	Description
Unicast	Enables aVCS Unicast election mode.
Mcast	Enables aVCS Multicast election mode.
Mixed	Enables both aVCS Multicast or Unicast election mode.

Default Mcast

Mode Global Config (vMaster or vBlade)

Usage This command is useful for establishing connectivity between L3 to L2 CGNAT nodes.

NOTE: If users only run “vcs discovery-mode Unicast”, then it removes avcs interface commands. If the “vcs discovery-mode mcast/vcs discovery-mode mixed”, then it reserves avcs interface commands.

Example The following commands configure aVCS to send its heartbeat to the multicast election address for 3 seconds. After supporting the unicast election, ACOS sends a heartbeat to the UDP unicast address. aVCS can also be running if ACOS is in a different subnet and there are routers inbetween them.

```
Ipv4 :
vrrp-a common
  device-id 2
```

```
  set-id 7
!
device-context 1
  vcs enable
!
device-context 2
  vcs enable
!

vcs device 2
  enable

vcs device 1
  enable
vcs unicast-election
  port 12000
  members
    ip-address 2.2.2.115
    ip-address 2.2.2.116

vcs discovery-mode Unicast

interface ethernet 1/2
  enable
  ip address 2.2.2.115 255.255.255.0

interface ethernet 2/2
  enable
  ip address 2.2.2.116 255.255.255.0

Ipv6:

vrrp-a common
  device-id 1
  set-id 7
!
device-context 1
  vcs enable
!
device-context 2
```

```
  vcs enable
!
vcs unicast-election
  port 12005
  members
    ipv6-address 3000::115 use-mgmt-port
    ipv6-address 3000::116 use-mgmt-port
!

vcs discovery-mode Unicast
multi-config enable
!
device-context 1
  interface management
    ip address 192.168.105.116 255.255.255.0
    ip default-gateway 192.168.105.1
    ipv6 address 3000::116/64
!
device-context 2
  interface management
    ip address 192.168.105.115 255.255.255.0
    ip default-gateway 192.168.105.1
    ipv6 address 3000::115/64
```

vcs enable

Description Enablea aVCS on the device.

Syntax **`vcs enable`**

Default N/A. This is an operational command rather than a configuration command.

Mode Privileged EXEC (vMaster or vBlade)

Usage After you enter the **`vcs enable`** command, you must enter the **`vcs reload`** command to place any aVCS configuration changes into effect and activate the feature.

Before using this command, many of the aVCS commands are not available from the CLI.

The following example shows the commands available prior to running the **vcs enable** command:

```
ACOS(config)# vcs ?
  failure-retry-count  VCS retry count after fails to join the
chassis
  vMaster-maintenance  During this period, vMaster can leave
and come back to
                       be vMaster again
  enable               enable VCS
  disable              disable VCS
ACOS(config)# vcs
```

In addition to enabling aVCS on the current device, you can also use device-context to enable aVCS on another device.

Example The following example enables aVCS on the current device:

```
ACOS-Active-vMaster[1/1]# vcs enable
ACOS-Active-vMaster[1/1]#
```

Example The following example switches to device 2 from device 1, then enables aVCS on device 2:

```
ACOS-Active-vMaster[1/1]# configure
ACOS-Active-vMaster[1/1](config:1)# device-context 2
All the following configuration will go to device 2
ACOS-Active-vMaster[1/1](config:2)# vcs enable
ACOS-Active-vMaster[1/1](config:2)#
```

vcs failure-retry-count

Description Configures the maximum number of retries for an aVCS device to join a virtual chassis.

Syntax

```
[no] vcs failure-retry-count {retries | forever}
```

Parameter	Description
retries	Maximum number of retries for an aVCS device to join a virtual chassis. You can specify 0-255.
forever	Specify an unlimited amount of retries for an aVCS device to join a virtual chassis.

Default 2

Mode Global Config (vMaster or vBlade)

Usage If the device is unable to join the virtual Multi-PU platform after all allowed retries are used, aVCS stops on the device. In this case, you use the **vcs reload** command to restart aVCS on the device.

Example The following command configures an ACOS Device to try 3 times to join a virtual chassis:

```
ACOS-Active-vMaster[1/1](config:1)# vcs failure-retry-count 3
```

vcs floating-ip

Description Configures the management IP address for the aVCS.

Syntax `[no] vcs floating-ip ipaddr {subnet-mask | /mask-length}`

Specifies the IP address and subnet mask.

Default Not set

Mode Global Config (vMaster or vBlade)

Example The following command sets the management address for the aVCS to **192.168.1.69/24**:

```
ACOS-Active-vMaster[1/1](config:1)# vcs floating-ip
192.168.1.69 /24
```

vcs floating-ipv6

Description Configures an IPv6 management IP address for the aVCS.

Syntax `[no] vcs floating-ipv6 ipv6-addr/mask-length`

Specifies the IP address and subnet mask.

Default Not set

Mode Global Config (vMaster or vBlade)

Example The following command sets the management address for the aVCS to the IPv6 address **fc00:0:3::23:a/24**:

```
ACOS-Active-vMaster[1/1](config:1)# vcs floating-ipv6
fc00:0:3::23:a/24
```

vcs force-wait-interval

Description Delays the start of aVCS following a reload or reboot.

Syntax `[no] vcs force-wait-interval seconds`

Replace *seconds* with the number of seconds (5-240) to wait following a reload or reboot to start aVCS.

Default 5

Mode Global Config (vMaster or vBlade)

Usage This command can be useful if you use staggered upgrade.

Example The following command configures the device to wait 10 seconds after reload or reboot:

```
ACOS-Active-vMaster[1/1](config:1)# vcs force-wait-interval 10
```

vcs hold-preemption-interval

Description Configures the number of seconds a device must wait before it starts challenging peers for the vMaster role.

Syntax `[no] vcs hold-preemption-interval <num>`

Replace *<num>* with the number of seconds (30-600) a device waits before challenging peers for the vMaster role.

Default 60

Mode Global Config (vMaster or vBlade)

Usage This command is available only on the chassis.

Example The following command configures the device to wait for 120 seconds before challenging peers for the vMaster role:

```
ACOS-Active-vMaster[1/1](config:1)# vcs hold-preemption-interval 120
```

vcs multicast-ip

Description Configures the multicast IPv4 address used for aVCS vMaster election.

Syntax

```
[no] vcs multicast-ip ipv4-addr
```

Replace *ipv4-addr* with the multicast address.

Default 224.0.1.210

Mode Global Config (vMaster or vBlade)

Usage The vcs multicast-port command is used to configure the protocol port.

Example The following command configures the multicast IPv4 address used for aVCS vMaster election:

```
ACOS-Active-vMaster[1/1](config:1)# vcs multicast-ip 224.0.1.210
```

vcs multicast-ipv6

Description Configures the multicast IPv6 address used for aVCS vMaster election.

Syntax

```
[no] vcs multicast-ip ipv6-addr
```

Replace *ipv6-addr* with the multicast address.

Mode Global Config (vMaster or vBlade)

Usage The vcs multicast-port command is used to configure the protocol port.

Example The following command configures the multicast IPv6 address used for aVCS vMaster election:

```
ACOS-Active-vMaster[1/1](config:1)# vcs multicast-ipv6 ff0e::100
```

vcs multicast-port

Description Configures the protocol port used for aVCS vMaster election.

Syntax

```
[no] vcs multicast-port portnum
```

Replace *portnum* with the protocol port number, 1-65535.

Default 41217

Mode Global Config (vMaster or vBlade)

Usage The vcs multicast-ip command is used to configure the multicast address.

Example The following command configures the protocol port used for aVCS vMaster election:

```
ACOS-Active-vMaster[1/1](config:1)# vcs multicast-port 41217
```

vcs offload upgrade protocol <scp>

Description Enables using the Secure Copy Protocol (SCP) for upgrade image transmission to member nodes in an aVCS cluster.

Syntax

```
[no] vcs offload upgrade protocol <scp>
```

Default Disabled

Mode Global Config (vMaster)

Usage This command supports all aVCS deployments such as multicast, unicast, IPv4, and IPv6. If it is not configured, the system uses the default method.

NOTE: The SSH service on the data port must be enabled on the VCS interface as the SCP protocol is used to transmit the upgrade image. By default, the SSH service is enabled on the management port. For more information, see enable-management.

Example The following command enables the transmission of the upgrade image to the node using SCP:

```
ACOS-Active-vMaster[1/1](config:1)# vcs offload upgrade protocol scp
```

Related Commands:

- enable-management

vcs reload

Description Reloads the aVCS process.

Syntax

```
vcs reload {cluster-discovery | db-safe start [timeout]| complete [force] | device | disable-merge}
```

Parameter	Description
cluster-discovery	The **cluster-discovery** option applies the configuration changes on the aVCS.
db-safe	During the vcs reload process, the **db-safe** option ensures that Scaleout is stable and the traffic is uninterrupted. • *start* - VCS enters the db-safe reload mode. In this mode, Scaleout remains stable and ignores any node leaving or joining. ◦ *timeout* - This option ends the db-safe mode based on the specified timeout value. The value

Parameter	Description
	can be 5-300 seconds. The expiration timeout is calculated based on the time when the new PU1 is elected. If the *vcs reload db-safe start* option is used without the timeout option, then the db-safe mode ends automatically after the vcs reload process completes. • *complete* - This option completes the db-safe reload mode. It must be used on PU1. ◦ *force* - This option completes the db-safe vcs reload within the specified timeout or after the timeout. **NOTE:** If, for any reason, the db-safe mode is not completed, you can use the *force* option to complete the db-safe mode forcefully.
device	The *device* option reloads a specific device when aVCS is enabled. The device ID can be between 1-16.
disable-merge	The **disable-merge** option prevents configuration information from being migrated from PU2 to PU1 following the reload. Use this option when you are replacing a virtual Multi-PU platform PU2 by removing an ACOS Device and replacing it with another ACOS Device of the same model. In this case, the option allows the replacement device to be configured by PU1. After the initial configuration migration, configuration synchronization operates normally. Without using this option, when you add an ACOS Device to a virtual Multi-PU platform that is already running, the device's configuration information is migrated to PU1.

Default N/A

Mode Global Config (PU1 only)

Usage VCS reload is required to place any aVCS-related configuration changes into effect.

Example The following command applies the configuration changes on the aVCS:

```
ACOS-Active-vMaster[1/1](config:1)# vcs reload cluster-discovery
```

vcs ssl-enable

Description Enables or disables SSL for configuration synchronization traffic between aVCS devices.

Syntax

```
[no] vcs ssl-enable
```

Default Disabled

Mode Global Config (vMaster only)

Example The following command enables SSL for configuration synchronization traffic between aVCS devices:

```
ACOS-Active-vMaster[1/1](config:1)# vcs ssl-enable
```

vcs time-interval

Description Configures number of seconds between keepalive messages from the vMaster to vBlades.

Syntax

```
[no] vcs time-interval seconds
```

Replace *seconds* with the number of seconds between transmission of keepalive messages from the vMaster to vBlades. You can specify 0-60 seconds.

Default 3

Mode Global Config (vMaster or vBlade)

Example The following command configures 12 seconds between transmission of keepalive messages from the vMaster to vBlades:

```
ACOS-Active-vMaster[1/1](config:1)# vcs time-interval 12
```

vcs time-interval-mseconds

Description Configures the number of milliseconds between keepalive messages from the vMaster to vBlades.

Syntax

```
[no] vcs time-interval-mseconds milliseconds
```

Replace *milliseconds* with the number of milliseconds between transmission of keepalive messages from the vMaster to vBlades. You can specify 200-900 milliseconds.

Default 0

Mode Global Config (vMaster or vBlade)

Example The following example sets the interval to 220 milliseconds:

```
ACOS-Active-vMaster[1/1](config:1)# vcs time-interval-mseconds
220
```

NOTE: For the `vcs dead-interval-mseconds` and the `vcs time-interval-mseconds` commands to work, you must configure in the following order:

```
vcs time-interval-mseconds 200
vcs dead-interval-mseconds 900
vcs time-interval 0
vcs dead-interval 0
```

vcs unicast-election

Description Configures the IPv4, IPv6, and protocol port used for aVCS unicast election.

Syntax

```
[no] vcs unicast-election
```

This command changes the CLI to the configuration level, where the following commands are available:

```
[no] members | port
```

This `members` command changes the CLI to the configuration level, to add the IPv4/IPv6 address of the member used for aVCS unicast election.

Command	Description
ip-address	Adds the IPv4 address of the member for aVCS unicast election.
ipv6-address	Adds the IPv6 address of the member for aVCS unicast election.

This `port` command configures the protocol port used for aVCS unicast election.

Command	Description
port	Configures the destination port for unicast election packet. The port can be 1025 to 65000. The default is 41217.

Mode Global Config (vMaster only)

Usage This command configures the IPv4, IPv6, and protocol port used for aVCS unicast election. By default, aVCS functions with Mcast discovery, you must use the `vcs discovery-mode Unicast` command to make it Unicast discovery.

Example The following commands configure the IPv4 address used for aVCS unicast election:

```
ACOS-Active-vMaster[1/1](config:1)#vcs unicast-election
ACOS-Active-vMaster[1/1](config:1-unicast-election)#members
ACOS-Active-vMaster[1/1](config:1-unicast-election-
members)#ip-address 192.168.1.1
ACOS-Active-vMaster[1/1](config:1-unicast-election-
members)#ip-address 192.168.1.2
```

```
ACOS-Active-vMaster[1/1](config:1-unicast-election-
members)#ip-address 192.168.1.3
```

Example The following commands configure the IPv6 address used for aVCS unicast election:

```
ACOS-Active-vMaster[1/1](config:1)#vcs unicast-election
ACOS-Active-vMaster[1/1](config:1-unicast-election)#members
ACOS-Active-vMaster[1/1](config:1-unicast-election-
members)#ip-address 2001:1:1:1::1
ACOS-Active-vMaster[1/1](config:1-unicast-election-
members)#ip-address 2001:1:1:1::2
ACOS-Active-vMaster[1/1](config:1-unicast-election-
members)#ip-address 2001:1:1:1::4
```

Example The following commands configure the protocol port number 41217 used for aVCS unicast election:

```
ACOS-Active-vMaster[1/1](config:1)# vcs unicast-election
ACOS-Active-vMaster[1/1](config:1-unicast-election)#port 41217
```

vcs vMaster-maintenance

Description Briefly place the vMaster into maintenance mode without triggering a failover to a vBlade.

Syntax `vcs vMaster-maintenance period`

Replace *period* with the amount of time (0-3600 seconds) that the vMaster is placed into maintenance mode without triggering a failover.

Default 60 seconds

Mode Global Config (vMaster or vBlade)

Usage The vMaster can be placed into maintenance mode without triggering a failover to a vBlade. During this maintenance window, the vBlades continue to operate without attempting to take over the vMaster role. At the end of the configurable maintenance period, the vMaster returns to the vMaster role.

vcs vmaster-take-over

Description Forces vMaster re-election, by temporarily changing a device's aVCS priority. This command is useful for changing a vBlade to vMaster without changing the aVCS configuration profile for either device.

Syntax

```
[no] vcs vmaster-take-over temp-priority
```

Replace *temp-priority* with the priority value, 1-255.

Default N/A

Mode Privileged EXEC (on vBlade); Privileged EXEC and Global Config (on vMaster)

Usage This command does not change the configured aVCS priority on the device. The command only temporarily overrides the configured priority.

If you enter this command on only one vBlade, you can specify any value within the valid range (1-255). The takeover occurs regardless of priority settings on the current vMaster.

If you enter the **vcs vmaster-take-over** command on more than one device, the device on which you enter the highest *temp-priority* value becomes the vMaster.

If you enter the same *temp-priority* value on more than one device, the same parameters used for initial vMaster election are used to select the new vMaster:

- The device with the highest configured aVCS priority is selected. (This is the priority configured by the **priority** command at the configuration level for the aVCS device.)
- If there is a tie (more than one of the devices has the same highest configured aVCS priority), then the device with the lowest device ID is selected.

In either case, the new vMaster is selected from among only the devices on which you enter the **vcs vmaster-take-over** command.

Example The following commands change the management context to a vBlade, then force the device to become the vMaster:

```
ACOS-1# vcs admin-session-connect device 2
spawn ssh -l admin 192.168.100.126
The authenticity of host '192.168.100.126 (192.168.100.126)'
can't be established.
RSA key fingerprint is
ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.126' (RSA) to the list
of known hosts.
Password:
Last login: Wed Aug 11 20:27:24 2010 from 192.168.3.74

[type ? for help]

ACOS>enable
Password:********
ACOS-2#vcs vmaster-take-over 255
```

Show Commands

show vcs debug

Description Displays aVCS debug messages.

Syntax `show vcs debug [old_first]`

Use the `old_first` option to list messages beginning with the most recent. Without this option, the list begins with the oldest message in the buffer.

Mode All

show vcs images

Description Displays the aVCS-capable software images stored on the ACOS Device.

NOTE: Only images that support aVCS are listed. To list all images, use the **show bootimage** command.

Syntax

```
show vcs images
```

Mode All

Example The following command shows the aVCS-capable software images stored on the device:

```
ACOS# show vcs images
Image Name                      Type
aximage_4_0_1_159.tar.gz        hd_pri
aximage_4_0_0_536.tar.gz        hd_sec
--------                        cf_pri
--------                        cf_sec
--------                        ext
```

The following table describes the fields in the command output:

Field	Description
Image Name	Name of the software image.
Type	Location of the image: • hd_pri – Primary image area of the hard drive or Solid State Drive (SSD) • hd_sec – Secondary image area of the hard drive or SSD • cf_pri – Primary image area of the compact flash drive • cf_sec – Secondary image area of the compact flash drive • ext – Extended image, used for staged upgrades during which multiple ACOS software versions run in the virtual chassis. **NOTE:** If dashes (--------) are displayed instead of an image name, the image does not support aVCS.

show vcs stat

Description Displays aVCS statistics information.

Syntax

```
show vcs stat
```

Mode All

Example The following command shows aVCS statistics information:

```
ACOS# show vcs stat

   Chassis-ID:                                8
   time-interval:                             3
   failure-retry-count:                       2
   force-wait-interval:                       5
   SSL-enabled:                               No
   Multicast-IP:                              224.0.0.210
   Multicast-Port:                            41217
   Unicast-elect-Port:                        12000
   Unicast-election-members:                  2
   Current discover mode : unicast
   Member-IP:                              192.168.105.127
   Member-IP:                              192.168.105.121
   Dev-ID:                                    1
      Dev-Prio:                               0
      Unicast-Port:                           41216
      Interfaces:                             management
      Enabled:                                Yes
   Local-Dev-ID:                              1
```

show vcs summary

Description Displays aVCS information.

Syntax

```
show vcs summary
```

Mode All

Example The following commands show the summary of the aVCS:

```
ACOS# show vcs summary

aVCS Chassis:
VCS Configuration-Sync Enabled:            Yes
VCS Database-distribution Enabled:         Yes (DB-SAFE-
RELOAD-MODE) [expire: 90 seconds]
Chassis ID:                                1
Floating IP:                               10.240.163.206
Mask:                                      255.255.255.240
Unicast Election port:                     12121
Multicast IP:                              224.0.1.210
Multicast Port:                            41473
Version:                                   6.0.1-d.b119
Current Discover mode:                     Unicast

Members (* means local device) (C:cfg-sync | D:db-sync |
B:both):
ID  State        PriorityIP:Port
        Location
-------------------------------------------------------------------
-----------------
1   vMaster(B)(*)125     172.16.10.100:41216
        Local
3   vBlade(B)    123     172.16.10.102:41216
        Remote
4   vBlade(B)    122     172.16.10.103:41216
        Remote
Total: 3
```

The following table describes the fields in the command output:

Field	Description
aVCS Chassis Fields	
VCS Configuration-Sync Enabled	Specifies the state of the aVCS configuration synchronization. • Yes - If it is enabled. • No - If it is disabled.

Field	Description
`VCS Database-distribution Enabled`	Specifies the state of the aVCS database-distribution. • Yes - If it is enabled. If it is runs in the db-safe mode, a message is displayed as DB-SAFE-RELOAD-MODE, along with the running timer or timeout. This message disappears after the db-safe mode ends. • No - If it is disabled.
`Chassis ID`	ID of the virtual chassis platform.
`Floating IP`	Floating IP of the virtual chassis platform.
`Mask`	Mask address of the virtual chassis platform.
`Unicast Election Port`	Unicast election port used for PU1 election.
`Multicast IP`	Multicast IP address used for PU1 election.
`Multicast Port`	Protocol port used for PU1 election.
`Version`	Software version and build running on the ACOS Device.
`Current discover Mode`	Specify Discover-mode as Unicast, Mcast, or Mixed election mode. To run unicast mode user must specify Discover-mode is Unicast (vcs discovery-mode Unicast) and provide Unicast neighbor configurations.
Members Fields	
`ID`	aVCS ID of the member device.
`State`	Current role of the device, vMaster or vBlade along with the status. • C - means configuration synchronization is active. • D - means database synchronization is active.

Field	Description
	• B - means both configuration and database synchronization are active. **NOTE:** If you enter this command in a session that is logged onto the aVCS floating IP address, the "local device" is always PU1, unless you change the context ID of the management session.
Priority	PU1 election priority of the device. **NOTE:** This is the admin-configured priority value, not the dynamic priority assigned by aVCS.
IP:Port	IP address and protocol port used for configuration synchronization with the member device.
Location	Indicates whether this is the device context on which you entered the **show vcs summary** command: • Local – This is the device context on which you entered the command. • Remote – This is not the device context on which you entered the command.

ACOS Virtual Router Redundant Protocol

VRRP-A is the ACOS implementation of high availability that is completely different from the industry-standard implementation of Virtual Router Redundancy Protocol (VRRP). For purposes of operational familiarity, it borrows concepts from VRRP but is significantly different from VRRP.

NOTE: VRRP-A will not inter-operate with VRRP.

This reference lists the CLI configuration and show commands that apply specifically to VRRP-A.

Configuration Commands

migrate-vip

Description Enable migration of all services from a particular virtual server located in a source VRRP-A pod to another virtual server located in a destination VRRP-A pod. This migration is independent of partitions and VRIDs. Service Migration occurs in a stateful process where all the sessions from the virtual server of the source VRRP-A pod are synced to a virtual server on the destination VRRP-A pod.

Syntax

```
migrate vip { cpu_number target_ip_address | cancel migration
| finish-migration }
```

Parameter	Description
cpu_number	Specify the target number of CPUs on the destination. The number ranges from 1 through 75.
target_ip_address	Specify the floating IPv4 or IPv6 address; it is the same address for the source and destination VRRP-A pods.
cancel	Cancel the migration.

Parameter	Description
migration	
finish migration	Finish the migration.

Default None

Mode Virtual server configuration mode

Usage Use this command to migrate a virtual server from a source VRRP-A pod to a destination VRRP-A pod. To qualify a VRRP-A pod for Service Migration as the destination pod, you must configure the destination pod with the same VIP, service groups, and route map as that of the source pod. If you cancel the migration, ensure that the OSPF cost metric on the source pod is made lower than that of the destination pod.

Example The following example initiates a migration to a destination VRRP-A pod:

```
ACOS1-Active(config-slb vserver)#migrate-vip 5 target-floating-ipv4 9.8.8.50
```

Example The following example cancels a migration:

```
ACOS1-Active(config-slb vserver)#migrate-vip cancel-migration
```

Example The following example finishes a migration:

```
ACOS1-Active(config-slb vserver)#migrate-vip finish-migration
```

vrrp-a common

Description Enter VRRP-A configuration mode, where additional VRRP-A commands are available.

Syntax **vrrp-a common**

Mode Global configuration mode

arp-retry

Description Specifies the minimum number of gratuitous Address Resolution Protocol (ARP) messages an ACOS device sends after transitioning from Standby to Active mode. These messages, also known as GARPs, are sent at regular intervals of 500 milliseconds.

Syntax

```
[no] arp-retry num
```

Default 4

Mode VRRP-A common configuration mode

Example Specifies the minimum number of gratuitous ARPs sent to 3 when the system becomes active.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# arp-retry 3
```

dead-timer

Description Changes the number of hello intervals during which a standby device will wait for a hello message from the Active VRRP-A device, before declaring the device to be down and beginning failover.

Syntax

```
[no] dead-timer num
```

Replace *num* with the maximum number of hello intervals to wait for a hello message.

Default 5 seconds

Mode VRRP-A common configuration mode

Example Set the number of hello intervals to 25.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# dead-timer 25
```

Related Commands:

- hello-interval

device-id

Description Specify the VRRP-A device ID of the device.

Syntax

```
[no] device-id num
```

Replace *num* with the device ID.

Mode VRRP-A common configuration mode

Usage If aVCS is configured, use the same number as the aVCS device ID.

Example Set the device ID to 7.

```
ACOS(config)# vrrp-a common
ACOS(config-common)#device-id 7
```

disable

Description Disable VRRP-A on the device.

This command replaces the **no enable** command in release 4.0.

Syntax

```
disable
```

Default By default, VRRP-A is disabled on any ACOS Device.

Mode VRRP-A common configuration mode

Example Disable VRRP-A on the device.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# disable
ACOS(config-common)
```

disable-default-vrid

Description Disable the default VRID on the shared partition.

Syntax

```
[no] disable-default-vrid
```

Default The default VRID is enabled by default.

Mode VRRP-A common configuration mode

Usage This command applies only to the shared partition.

Example Disable the default VRID on the shared partition.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# disable-default-vrid
```

enable

Description Enable VRRP-A on the device.

Syntax

```
enable
```

Default By default, VRRP-A is disabled on any ACOS Device.

Mode VRRP-A common configuration mode

Example Enable VRRP-A on the device.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# enable
ACOS-Active(config-common)#
```

forward-l4-packet-on-standby

Description Enable Layer 2/3 forwarding of Layer 4 traffic on the Standby ACOS Device.

Syntax

```
forward-l4-packet-on-standby
```

Default Disabled

Mode VRRP-A common configuration mode

Usage This command applies only to the shared partition.

Example Enable Layer 4 traffic forwarding on the device.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# forward-l4-packet-on-standby
```

get-ready-time

Description Configures a delay time interval in 100-millisecond intervals for VRRP-A starting to run after system start-up.

Syntax

```
[no]get-ready-time 100-ms-units
```

Default 6 seconds

Mode VRRP-A common configuration mode

Usage This command applies only to the shared partition.

Example Set the delay interval to 20 seconds (200-millisecond units).

```
ACOS(config)# vrrp-a common
ACOS(config-common)# get-ready-time 200
```

hello-interval

Description Change the interval at which the active device sends VRRP-A hello messages out its VRRP-A interfaces.

Syntax

```
[no] hello-interval 100-ms-units
```

Replace *100-ms-units* with the number of 100 ms (milliseconds) intervals between each hello message.

Mode VRRP-A common configuration mode

Example Set the hello interval to 4 (400 milliseconds).

```
ACOS(config)# vrrp-a common
ACOS(config-common)# hello-interval 4
```

hop-limit

Description Limit the number of hops for IPv6 unicast VRRP-A hello and session synchronization packets to prevent loops.

Syntax

```
[no] hop-limit num
```

Replace *num* with the desired value (0-255).

Mode VRRP-A common configuration mode

Example The following example enables the number of hops for IPv6 unicast VRRP-A.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# hop-limit 64
```

hostid-append-to-vrid

Description This command enables you to identify the members of the VRRP-A set by serial number.

The show vrrp-a hostid command can be used to view the serial number of each device in the VRRP-A set. By default, these serial numbers, which act as unique identifiers for all devices in the VRRP-A set, are included in the VRRP-A hello packets for all VRIDs.

This command causes the device serial numbers to be sent in the VRRP-A hello packets for the specified VRID only.

Syntax

```
[no] hostid-append-to-vrid {default | vrid-num}
```

Parameter	Description
`default`	VRID 0.
vrid-num	A non-0 VRID.

Mode VRRP-A common configuration mode

Example Device serial numbers should be included in the hello packets for VRID 3 only:

```
ACOS(config)# vrrp-a common
ACOS(config-common)# hostid-append-to-vrid 3
```

Related Commands:

- show vrrp-a hostid

inline-mode

Description Enable a specified ethernet port or trunk to be in Layer 2 inline hot standby mode.

Inline deployment allows you to insert a pair of ACOS Devices into an existing network without the need to reconfigure other devices in the network.

Inline support applies specifically to network topologies where inserting a pair of ACOS switches would cause a Layer 2 loop.

Syntax `[no] inline-mode {preferred-portport | preferred-trunktrunk}`

Parameter	Description
port	Ethernet port number.
trunk	Trunk number.

Default Not configured.

Mode VRRP-A common configuration mode

Example Configure ethernet port 2 as the port to be used in the inline deployment:

```
ACOS(config)# vrrpa-a common
ACOS(config-common)# inline-mode preferred-port 2
```

preemption-delay

Description Configure a delay between VRRP-A configuration changes and the time that preemption will take effect.

Syntax `[no] preemption-delay 100-ms`

Replace *100-ms* with the number of 100-millisecond units to wait before having preemption take effect.

Mode VRRP-A common configuration mode

Example Configure a preemption delay of 20 seconds (200 100-millisecond units).

```
ACOS(config)# vrrp-a common
ACOS(config-common)# preemption-delay 200
```

restart-time

Description The amount of time for ports on the standby system to be restarted after the transition from the standby mode to active mode.

Syntax `[no] restart-time seconds`

Replace *seconds* with the number of seconds.

Mode VRRP-A common configuration mode

Usage This command applies only to VRRP-A interfaces in a restart port list configured by the vrrp-a restart-port-list command.

set-id

Description Specify the VRRP-A set ID. When the set-id is "0", the set-id is not configured. To return to the default setting, use the `no` command.

Syntax

```
[no] set-id num
```

Replace *num* with the set ID.

Default This is not set by default, by using the value 0.

Mode VRRP-A common configuration mode

Example Configure a set ID of 4.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# set-id 4
```

track-event-delay

Description . Prevents failover flapping caused by brief, temporary link, or server health changes, on a single device when interface states change rapidly (UP or DOWN events occurring in quick succession). VRRP-A uses track event delay. The track event delay is the number of seconds a failover-causing event must persist before a failover occurs.

Syntax

```
[no] track-event-delay 100-ms-units
```

Replace *100-ms-units* with the number of milliseconds (ms) to wait before beginning failover.

Mode VRRP-A common configuration mode

Example Configure a delay of 5 seconds.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# track-event-delay 50
```

In this example, the track event delay is set to 5 seconds, and if a tracked link goes down for 3 seconds, then comes up, no failover is

triggered. Failover is triggered only if the link is down for at least 5 seconds.

ttl

Description Limit the number of hops for IPv4 unicast VRRP-A hello and session synchronization packets to prevent loops.

Syntax

```
[no] ttl num
```

Replace *num* with the desired TTL value (0-255).

Mode VRRP-A common configuration mode

Example The following example enables the number of hops for IPv4 unicast VRRP-A.

```
ACOS(config)#  vrrp-a common
ACOS(config-common)# ttl 128
```

vrrp-a fail-over-policy-template

Description Create a failover policy template for VRRP-A. The template provides a mechanism for event tracking and can enable a policy-based failover to occur. Using a template, assign weight-related values per event that will be reduced from the fixed total weight of an ACOS Device of 65534. The weight of a device can determine whether the device will serve as an Active or Standby device. This command allows you to specify the weight value per event that may cause a device to failover when the event occurs.

Syntax

```
[no] vrrp-a fail-over-policy-template template-name
```

Replace *template-name* with the name that you are assigning for the VRRP-A failover policy template. This template must be associated with a particular VRID to take effect.

This command changes the CLI to the configuration level for the specified failover-policy template, where the following commands are available.

Command	Description
[**no**] **gateway** *gateway-IP-address* **weight** *value*	Specify the IP Address of an IPv4 or IPv6 default gateway that has also been configured as a real server, such as `ACOS(config)#slb server GW1` or `ACOS(config)#cgnv6 server GW1`. VRRP-A periodically tests the status of the IP. If a gateway stops responding, VRRP-A reduces the weight for the VRID. The weight value to subtract can be specified individually for each gateway's IP address that you configure in the tracking events list.
[**no**] **interface** *interface-type interface-number* **weight** *value*	Specify a weight for each interface that you are planning to track. If the link goes down on an Ethernet data port, VRRP-A reduces the weight for the VRID. The weight value to subtract can be specified individually for each Ethernet data port.
[**no**] **route** **route-number** *subnet* **weight** *value* [**distance** *num*] [**gateway** *ip*] [**protocol** {**any** | **static** | **dynamic**}]	Indicate the IPv4 or IPv6 route that you wish to track. If the route matching the specified options is not in the data route table, VRRP-A reduces the weight for the VRID. The **distance** parameter specifies the route's administrative distance; if not specified, any distance is matched. The **gateway** parameter matches the route's next-hop gateway. The **protocol** parameter matches the route protocol: • **any** - match any routing protocol (default) • **static** - match only user-specified static routes • **dynamic** - match only routes added by dynamic routing protocols (for example, OSPF)

Command	Description
[**no**] **trunk** *trunk-id* **weight** *value* **per-port-weight** *value*	Indicate the trunk you wish to track. If the trunk or individual ports in the trunk go down, VRRP-A reduces the weight for the VRID. The weight value to subtract can be specified for the trunk and individual ports within the trunk.
[**no**] **vlan** *vlan-id* **timeout** *timeout-value* **weight** *value*	Indicate the VLAN you wish to track. If VRRP-A stops detecting traffic on a VLAN, VRRP-A reduces the weight for the VRID. The weight value to subtract can be specified individually for each VLAN.

Default None

Mode Global configuration mode

Usage Use this command on any ACOS Device to indicate weight values per tracked event via a failover policy template.

Example The following commands help you to create a template called "template1" and specify events that will reduce the weight of the VRID:

```
ACOS(config)# vrrp-a fail-over-policy-template template1
ACOS(config-fail-over-policy-template:tem...)# interface
ethernet 1 weight 200
ACOS(config-fail-over-policy-template:tem...)# gateway
20.20.20.20 weight 200
ACOS(config-fail-over-policy-template:tem...)# vlan 10 timeout
2 weight 200
ACOS(config-fail-over-policy-template:tem...)# route
20.20.20.0 /24 weight 200
ACOS(config-fail-over-policy-template:tem...)# trunk 1 weight
200
```

vrrp-a force-self-standby

Description Force the ACOS Device to change from active to standby or backup.

Syntax

```
[no] vrrp-a force-self-standby [all-partitions | vrid num]
{enable | disable}
```

Parameter	Description
all-partitions	Causes all partitions to change to a standby state.
vrid *num*	Causes only the specified VRID to change to a standby state.
enable	Enable the forced standby.
disable	Disable the forced standby.

Default N/A

Mode Global configuration mode

Usage This command provides a simple method to force a failover, without the need to change VRRP-A configuration settings.

Example Enable the forced standby of VRID 3:

```
ACOS(config)# vrrp-a force-self-standby vrid 3 enable
Doing so may cause some of the VRID(s) to become inactive in
the whole vrrp-a set.
WARNING: Please confirm that you want to perform this
operation.
Doing so may cause some of the VRID(s) to become inactive in
the whole vrrp-a set; make sure you verify that an active
device will be available after performing this operation.
[yes/no]:
```

vrrp-a force-self-standby-persistent

Description Force a specific VRID to change from active to standby or backup and remain in the backup state even after the device is reloaded.

Syntax

```
[no] vrrp-a force-self-standby-persistent [vrid num]
```

Replace *num* with the VRID number whose state you want to change.

Default N/A

Mode Global configuration mode

Usage This command provides a simple method to force a failover, without the need to change VRRP-A configuration settings.

Example Enable the persistent forced standby of VRID 3:

```
ACOS(config)# vrrp-a force-self-standby-persistent vrid 3
Doing so may cause some of the VRID(s) to become inactive in
the whole vrrp-a set.
WARNING: Please confirm that you want to perform this
operation.
Doing so may cause some of the VRID(s) to become inactive in
the whole vrrp-a set; make sure you verify that an active
device will be available after performing this operation.
[yes/no]:
```

vrrp-a interface

Description Configure a VRRP-A interface.

Syntax

```
[no] vrrp-a interface {ethernet port-num | trunk trunk-num}
```

Parameter	Description
port-num	Configures the specified interface as the VRRP-A interface.
trunk-num	Configures the specified trunk interface as the VRRP-A interface.

This command places you in a configuration sub-mode where you can configure the type and state of the interface using the following commands:

Command	Description
no-heartbeat	Prevents heartbeat packets from being sent out on this interface.
vlan *vlan-id*	Configures the interface to be part of the specified VLAN.

Default All Up data interfaces within a partition are VRRP-A interfaces for that partition. If an interface is a tagged member of multiple VLANs, only the VLAN that has the lowest VLAN ID for the interface is used as a VRRP-A interface.

Mode Global configuration mode

Usage This command is valid only in the shared partition. However, the interface(s) specified by the command is used by all partitions.

Example Configure ethernet interface 3 as the VRRP-A interface, and configure the interface so that real servers can be reached:

```
ACOS(config)# vrrp-a interface ethernet 3
ACOS(config-ethernet:3)# vlan 13
```

vrrp-a l2-inline-peer-ip

Description Configure a peer IP address in Layer 2 inline mode HA deployments.

ACOS Devices require a connection mirror IP address to be configured in Layer 2 inline mode VRRP-A deployments. A connection mirror interface is a unicast IP address on the peer ACOS Device in the VRRP-A set. This peer IP address is optional in earlier releases but usually is configured anyway for session synchronization purposes. Specifying a connection mirror IP address is mandatory for proper operation of ACOS Devices in Layer 2 Inline mode VRRP-A.

The connection mirror IP address is used for session synchronization (also called “connection mirroring”). Until a connection mirror IP address is specified, the ACOS Device remains in a Standby state.

If a connection mirror IP address is not configured, a log message such as the following is generated every 5 minutes:

```
Sep 01 2012 03:01:30 Warning [HA]:HA Peer IP is not
configured. Peer IP is required in Inline Mode.
```

Syntax `[no] vrrp-a l2-inline-peer-ip ip-address`*ipaddr*

Default Not configured

Mode Global configuration mode

Example Configure 192.168.1.1 as the peer IP address.

```
ACOS(config)# vrrp-a l2-inline-peer-ip ip-address 192.168.1.1
```

vrrp-a l3-inline-mode

Description Enable Layer 3 Inline mode.

Syntax `[no] vrrp-a l3-inline-mode`

Default Not configured

Mode Global configuration mode

Example Enable Layer 3 inline mode.

```
ACOS(config)# vrrp-a l3-inline-mode
```

vrrp-a ospf-inline

Description Enable OSPF inline mode.

Syntax `[no] vrrp-a ospf-inline vlan` *vlan-id*

Replace *vlan-id* (1-4094) with the VLAN for which you do not want to filter OSPF packets.

Default Not enabled

Mode Global configuration mode

Example Enable OSPF inline mode and do not filter packets on VLAN 13.

```
ACOS(config)# vrrp-a ospf-inline vlan 13
```

vrrp-a peer-group

Description Configure a VRRP-A peer group. This allows you to configure unicast IP/IPv6 addresses through a layer 3 link (Layer 3 inline mode). Heartbeat messages are routed to the destination.

Syntax

```
[no] vrrp-a peer-group
```

This command places you in a sub-configuration mode, where you can configure the peer address with the **peer** command:

```
[no] peer {ipv4-address | ipv6-address}
```

Replace *ipv4-address* or *ipv6-address* with the appropriate IP address of the peer.

Mode Global configuration mode

Example The following example shows how to configure a peer group:

```
ACOS(config)# vrrp-a peer-group
ACOS(config-peer-group)# peer 192.168.10.10
ACOS(config-peer-group)# peer 30.20.10.6
ACOS(config-peer-group)# peer 2607:f0d0:1002:51::4
```

vrrp-a preferred-session-sync-port ethernet

Description Specify the Ethernet interfaces on which to receive synchronized sessions.

Syntax

```
[no] vrrp-a preferred-session-sync-port {
ethernet port-num [vlan vlan-id]
trunk trunk-num [vlan vlan-id]
}
```

Parameter	Description
port-num	Configure the specified ethernet port to receive sync sessions.
trunk-num	Configure the specified trunk port to receive sync sessions.
vlan-id	If your interface is part of a VLAN, specify the VLAN ID.

Default The default behavior is for VRRP-A (on the backup device) to automatically select the Ethernet interface on which to receive sync sessions.

Mode Global configuration mode

Example Configure trunk 3 to receive sync sessions.

```
ACOS(config)# vrrp-a preferred-session-sync-port trunk 3
```

vrrp-a restart-port-list

Description Causes the ports on the standby system to be restarted after the transition from the standby mode to active mode.

Beginning with release 4.0.1, you can configure the restart time using restart-time.

Syntax

```
[no] vrrp-a restart-port-list
```

This command places you in a sub-configuration mode where the following commands are available:

Command	Description
ethernet {*port* | *range_of_ports*}	Configure one or many VRRP-A interface ports to restart.
vrid *num*	Enters a VRID sub-configuration mode where the ethernet port or range is also available:

Command	Description
	ACOS(config-restart-port-list)# **vrid 1** ACOS(config-restart-port-list-vrid:1)#

NOTE: You must omit at least one port connecting the ACOS Devices from the restart port-list, and heartbeat messages must be enabled on the port. This is so that heartbeat messages between the ACOS Devices are maintained; otherwise, flapping might occur.

Mode Global configuration mode

Default Disabled. VRRP-A interfaces are not restarted after a failover.

Usage Use this command in inline mode configurations to cause the router connected to the ACOS Device to relearn MACs, including MACs for the real servers. Without this command, the router might continue to try to reach the real servers through the ACOS Device that becomes the Standby ACOS Device after a failover.

VRRP-A port restart toggles a specified set of ports on the formerly Active ACOS Device by disabling the ports, waiting for a specified number of milliseconds, then re-enabling the ports. Toggling the ports causes the links to go down, which in turn causes the devices on the other ends of the links to flush their learned MAC entries on the links. The devices then can relearn MACs through links with the newly Active ACOS Device.

vrrp-a vrid

Description Access the configuration level for a VRID.

Syntax

```
[no] vrrp-a vrid num
```

Specify the VRID ID number. The number of VRIDs available for configuration differs in shared versus L3V partitions.

This command changes the CLI to the configuration level for the specified VRID.

The commands available at this level are:

- blade-parameters
- floating-ip
- follow
- preempt-mode

Mode Global configuration mode

vrrp-a vrid-lead

Description Configures a VRID as the “leader” VRID, with other VRIDs to operate as followers.

Syntax

```
[no] vrrp-a vrid-lead name
```

Replace *name* with the name of the VRID.

This command changes the CLI to the configuration level for the specified VRID leader, where the following command is available:

[no] partition [shared | name] vrid *ID-num*

This command designates this VRID as the leader for a specific partition.

Default Not set

Mode Global configuration mode

Usage For the leader VRID only, you can configure all capabilities, such as configuring the failover policy template, the preempt mode, priority, and tracking options. For follower VRIDs, you can only configure Floating IP Addresses.

If you try to remove a VRID that is configured as a lead VRID and that has other VRIDs that follow it, you will not be allowed to remove it. You must remove the VRIDs that are configured as followers before you remove the lead VRID.

Example The following command configures a VRID lead in the shared partition:

```
ACOS(config)# vrrp-a vrid-lead lead1
ACOS(config-vrid-lead)# partition shared vrid 1
```

vrrp-a session-sync

Description Configure vrrp-a session- sync to enable or disable the session synchronization.

Syntax

```
[no] vrrp-a session-sync
```

This command allows to enable or disable the session sync on a per partition basis. Enable/disable session sync for private partition can only be done from CLI.

Default Enabled

Mode Global configuration mode

Usage User may control the session synchronization on the shared partition or private partitions. Once the CLI is enabled, the session synchronization will be in force from the VRRP-A active to the VRRP-A standby. The user may also disable the session synchronization on a per-partition basis

Example The following command configures a session-sync in the shared partition:

```
vThunder-Active(config-)# vrrp-a session-sync
enable enable vrrp-a session sync
disable disable vrrp-a session sync
vThunder-Active(l3v)# vrrp-a session-sync
enable enable vrrp-a session sync
disable disable vrrp-a session sync
```

vrrp-a vrid

Description Access the configuration level for a VRID.

Syntax

```
[no] vrrp-a vrid num
```

Specify the VRID ID number. The number of VRIDs available for configuration differs in shared versus L3V partitions.

This command changes the CLI to the configuration level for the specified VRID.

The commands available at this level are:

- blade-parameters
- floating-ip
- follow
- preempt-mode

Mode Global configuration mode

blade-parameters

Description Enters vBlade configuration mode.

Commands available for configuring blade parameters are:

- fail-over-policy-template
- priority
- tracking-options

Syntax

```
[no] blade-parameters
```

Mode VRRP-A VRID configuration mode
VRRP-A VRID configuration mode is accessed by entering the vrrp-a vrid command. For example,

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)#
```

Example Enter Vblade configuration mode:

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)# blade-parameters
ACOS(config-vrid:0-blade-parameters)#
```

floating-ip

Description Specifies the IP addresses that downstream devices should use as their default IPv4 or IPv6 gateways. Regardless of which device is active for the VRID, downstream devices can reach their default IPv4 or IPv6 gateway at the floating IP address.

Syntax

```
[no] floating-ip {ipaddr | ipv6addr [ethernet id | trunk id | ve id]}
```

Parameter	Description
ipaddr	The IPv4 address of the floating IP.
ipv6addr	The IPv6 address of the floating IP. • `ethernet id` - Ethernet interface. Visible in the shared partition. • `trunk id` - Trunk interface. Visible in the shared partition. • `ve id` - Virtual Ethernet interface. Visible in the shared partition.

Default N/A

Mode VRRP-A VRID configuration mode

Example The following example configures 10.10.10.8 as the floating IP address for the VRID:

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)# floating-ip 10.10.10.8
```

follow

Description Configure a follower VRID.

Prerequisite Before you can use this command, you must have configured a leader VRID using the vrrp-a vrid-lead command.

NOTE: This command only appears in an L3V partition; it does not appear in the shared partition.

Syntax

```
[no] follow vrid-lead name
```

Replace *name* with the name of the leader VRID.

Mode VRRP-A VRID configuration mode

Example This example shows how to follow the lead VRID called “lead1” from the shared partition “p1” on VRID 1:

```
ACOS(config)# active-partition p1
Current active partition: p1
ACOS[p1](config)# vrrp-a vrid 1
ACOS[p1](config-vrid:1)# follow vrid-lead lead1
```

preempt-mode

Description Disables ability for failovers to be caused by priority value changes, including manually changed priority values or any VRID tracking-option events.

Syntax

```
[no] preempt-mode {disable | threshold num}
```

Parameter	Description
disable	Disables preempt mode.
threshold *num*	Controls whether failovers can be caused by priority value changes. The threshold specifies the maximum difference in priority value that can exist between the active and standby devices without failover occurring. The default is 0.

Default Preemption is enabled by default.

Mode VRRP-A VRID configuration mode

Example The following example disables preemption:

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)# preempt-mode disable
```

NOTE: When preempt mode is enabled and ACOS device becomes ready to process traffic after reload/reboot/power-on, ACOS device keeps standby status for 6 seconds if heartbeat keep-alive messages are received from peer active ACOS device. This timer is held because the standby ACOS device may need to synchronize sessions from the active device before trying to become active.

blade-parameters

Description Enters vBlade configuration mode.

Commands available for configuring blade parameters are:

- fail-over-policy-template
- priority
- tracking-options

Syntax

```
[no] blade-parameters
```

Mode VRRP-A VRID configuration mode
VRRP-A VRID configuration mode is accessed by entering the vrrp-a vrid command. For example,

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)#
```

Example Enter Vblade configuration mode:

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)# blade-parameters
ACOS(config-vrid:0-blade-parameters)#
```

fail-over-policy-template

Description Specify the name of the vrrp-a fail-over-policy-template and apply to the VRID.

Syntax

```
[no] fail-over-policy-template template-name
```

Mode VRRP-A Blade parameter configuration mode

Example The following example applies the policy template named “template1” to VRID 0:

```
ACOS(config)#vrrp-a vrid 0
ACOS(config-vrid:0)#blade-parameters
ACOS(config-vrid:0-blade-parameters)#fail-over-policy-template template1
```

priority

Description Specifies the preference of the device to become the active device for the VRID. The device that has the highest priority value for the VRID becomes the active device for the VRID.

Syntax

```
[no] priority num
```

Replace *num* with the desired priority.

Default 150

Mode VRRP-A Blade parameter configuration mode

Usage This command is changed from release 4.0, where it was available under VRRP-A VRID configuration mode.

Example The following example sets the priority on VRID 0 to 200:

```
ACOS(config)#vrrp-a vrid 0
ACOS(config-vrid:0)#blade-parameters
ACOS(config-vrid:0-blade-parameters)#priority 200
```

tracking-options

Description Accesses the configuration level for tracking options. Tracking options can dynamically reduce the priority value used in dynamic failover.

Syntax

```
[no] tracking-options
```

The supported tracking options are summarized in the table below.

Option	Syntax	Description
Gateway	[**no**] **gateway** {*ipaddr* | *ipv6addr*} **priority-cost***num*	Configure tracking for the IPv4 or IPv6 default gateways. If a gateway fails, the specific *num* will be subtracted from the priority on the VRID.
Interface	[**no**] **interface ethernet** *num* **priority-cost***num*	Configure tracking for a specified interface. If the interface fails, the specific *num* will be subtracted from the priority on the VRID.
Route	[**no**] **route** {*ipaddr* | *ipv6addr*} {**/***mask-length* | *subnet-mask*} [**priority-cost***num*] [**distance** *num*] [**gateway***ip*] [**protocol** {**any** | **static** | **dynamic**}]	Configure tracking for the specified route. If the specified route is missing, the specific *num* will be subtracted from the priority on the VRID. The **distance** parameter specifies the route's administrative distance; if not specified, any distance is matched. The **gateway** parameter matches the route's next-hop gateway. The **protocol** parameter matches the route protocol: • **any** - match any routing protocol (default) • **static** - match only user-specified static routes • **dynamic** - match only routes added by dynamic routing protocols (for example, OSPF)

Option	Syntax	Description
Trunk	[**no**] **trunk** *num* **priority-cost***num* [**per-port-pri***num*]	Configure tracking for a specified trunk. If the trunk or individual ports on the trunk fail, the specified priority cost *num* will be subtracted from the priority on the VRID. The **per-port-pri** option tracks individual ports in the trunk. The VRID's priority is reduced by the **per-port-pri** amount for each port that fails.
VLAN	[**no**] **vlan***vlan-id* **timeout** *seconds* **priority-cost***num*	Configure tracking for the specified VLAN. If traffic is no longer detected on the specified VLAN, the specific *num* will be subtracted from the priority on the VRID. The **timeout** option configures the number of seconds a VLAN can remain idle without triggering a failover and priority cost reduction.

Default N/A

Mode VRRP-A Blade parameter configuration mode

Usage This command is changed from release 4.0, where it was available under VRRP-A VRID configuration mode.

Example

```
ACOS(config)# vrrp-a vrid 0
ACOS(config-vrid:0)# blade-parameters
ACOS(config-vrid:0-blade-parameters)# tracking-options
```

Show Commands

show vrrp-a

Description Displays VRRP-A information.

Syntax

```
show vrrp-a [detail]
```

Mode All

Usage This command is only valid in the shared partition.

Example The following example shows sample output for the `show vrrp-a` command.

```
ACOS# show vrrp-a
vrid 0
Unit State Weight Priority IP
1 Local Standby 65385 150 N/A
became Standby at: [IST] Wed, 26-Apr-2023 23:33:32 for 11
Days, 22 Hours, 20 Mins
2 (Peer) Active 65534 150 22.22.22.21
3 (Peer)* Standby 65534 150 aa:aa:aa:aa:aa:aa:aa:23
Switch to active 0, switch to standby 0
Detected local policy based fail over events:
          gateway 22.22.22.21 weight 45
          gateway f4::bb weight 32
          gateway 45:ee:ff:91:a1:4f:23:9c weight 2
          route 222.222.222.0 255.255.255.0 gateway 3.3.3.3
distance 30 protocol dynamic weight 33
          route ff::/16 weight 22
          route aa::/16 gateway aa:aa:aa:aa:aa:aa:aa:aa
distance 56 protocol static weight 6
          bgp 3c:: weight 9
```

```
Hello Packet Counters          Peer 2       Peer 3    All Peers
                              RX/Miss      RX/Miss           TX
Port 3:                     2972826/0          0/0      2972818
Port 4:                     2972826/0    2972780/0      2972818
Totals:                     5945652/0    2972780/0      5945636

vrid 1
Unit State Weight Priority IP
1 (Local) Active 65534 150 N/A
became Active at: [IST] Mon, 01-May-2023 22:21:07 for 6 Days,
23 Hours, 32 Mins
2 (Peer)* Standby 65534 150 22.22.22.21
Switch to active 0, switch to standby 0
Hello Packet Counters          Peer 2    All Peers
                              RX/Miss           TX
Port 3:                     2972826/0      2972818
Port 4:                     2972826/0      2972818
Totals:                     5945652/0      5945636


Hello Packet Counters          Peer 2       Peer 3
Total RX:                    11891304      2972780
```

```
Conn Sync Pkts:                          Sent       0
Received       0
-------------------------------------------------------------
---------------
Conn Sync Create Session:                Sent       0
Received       0
Conn Sync Update Age:                    Sent       0
Received       0
Conn Sync Delete Session:                Sent       0
Received       0
Conn Sync Create Persist Session:        Sent       0
Received       0
Conn Sync Update Persist Age:            Sent       0
Received       0
Conn Sync Delete Persist Session:        Sent       0
Received       0
Conn Sync Update LSN RADIUS:             Sent       0
Received       0
Conn Sync Update LSN Fullcone:           Sent       0
Received       0
Conn Sync Acos Monitoring Entities:      Sent       0
Received       0

Dup device id:     0          Set id mismatch:     0
Version mismatch:  0          Error partition id:  0
Error port:        0          Error device id:     0
Lock:              0          Time inaccuracies:   0
IP pools exceeded: 0          IPv6 pools exceeded: 0
L2 no route:       0
```

The fields in this output are described in the following table:

Field	Description
vrid	Virtual router ID.
Unit	VRRP-A device ID. “Local” indicates this ACOS device. “Peer” indicates another ACOS device in the same

Field	Description
	VRRP-A set.
State	VRRP-A state: • Active • Standby
Weight	Current VRRP-A weight of this device.
Priority	Current VRRP-A priority of this device.
vrid that is running	VRID that is currently running on the partition.
VRRP-A Stats The following information is listed for each VRRP-A peer device.	
Peer	Device ID of the peer device, and the VRID.
Port	Data port that connects this device (the Local device) to the peer device. The received counter indicates the number of Hello packets received for the VRID from the peer on this port. The missed counter indicates the number of Hello packets that were expected for the VRID but did not arrive from the peer on this port.
Heartbeat missed	Number of Hello packets that were expected for the VRID from the peer but did not arrive on any port.
Total packets received from peer	Total number of Hello packets received from the peer.
Detail Fields **NOTE:** The following fields appear only if you use the detail option.	
Conn Sync Pkts	Number of connection (session) synchronization packets sent by this partition

Field	Description
	for the VRID.
Conn Query Pkts	Number of session synchronization query packets sent by this partition for the VRID. Query packets are sent by the standby device to request session information.
Conn Sync Create Session Pkts	Number of creation packets for synchronized connections sent by this partition for the VRID.
Conn Sync Update Age Pkts	Number of update packets for synchronized connections sent by this partition for the VRID.
Conn Sync Delete Session Pkts	Number of delete packets for synchronized connections sent by this partition for the VRID.
Total packets sent for vrid N	Total number of Hello packets sent by this partition for the VRID. Separate counters are listed for each data port used by this partition to send the packets.
Dup device ID	Number of incoming hello packets that had the same device ID as this device (the local device).
Set ID mismatch	Number of incoming hello packets in which the VRRP-A set ID was different from this device's set ID.
Version mismatch	Number of incoming hello packets that had a different VRRP-A software version than the one running on this device.
Error port	Number of hello messages received from a non-existent port.
Error device ID	Number of hello messages received from an invalid device ID (any device ID higher than 8).
Switch to active, switch to	Number of times the partition transitioned to Active or Standby for the VRID.

Field	Description
standby	
Peer IP	IP address of the active peer for the VRID. The active peer is the device to which this device (the local device) sends sessions for synchronization.

show vrrp-a all-partitions

Description View VRRP-A information for all partitions.

Syntax

```
show vrrp-a all-partitions [active]
```

Parameter	Description
active	Show only active VRIDs in the output.

Mode All

Usage This command is only valid in the shared partition.

Example Example output for this command:

```
ACOS# show vrrp-a all-partitions
Local device ID: 1
Partition vrid  Active(P,W)          Standby(P,W)
shared  0       2 (150,65534)        1 (11,65534)
a       0       1 (150,65534)        2 (150,65534)
```

The fields in this output are described in the following table:

Field	Description
Local device ID	Device ID of the device on which this command was executed.
Partition	Name of the partition.
vrid	VRID configured in the partition.

Field	Description
Active (P,W)	Device number, priority (P), and weight (W) of the active device in the VRID. For example: `2 (150,65534)` means the active device is device 2, the priority is 150, and the weight is 65534.
Standby (P,W)	Device number, priority (P), and weight (W) of the standby device in the VRID.

show vrrp-a fail-over-policy-template

Description Display the VRRP-A fail-over policy template details.

Syntax

```
show vrrp-a fail-over-policy-template [template_name]
```

Mode All

Example The following command shows VRRP-A information for all the fail-over policy templates:

```
ACOS(config)# show vrrp-a fail-over-policy-template
vrrp-a fail-over-policy-template interface
   interface ethernet 1 weight 200
vrrp-a fail-over-policy-template trunk
   trunk 1 priority-weight 200
vrrp-a fail-over-policy-template gateway
   gateway 41.41.41.20 weight 200
   gateway 20.20.20.20 weight 50
vrrp-a fail-over-policy-template route
   route 4.4.4.0 255.255.255.0 weight 200
vrrp-a fail-over-policy-template vlan
   vlan 10 timeout 2 weight 200
vrrp-a fail-over-policy-template template1
   interface ethernet 1 weight 200
   gateway 20.20.20.20 weight 200
   vlan 10 timeout 2 weight 200
   trunk 1 priority-weight 200
   route 20.20.20.0 255.255.255.0 weight 200
```

If you specify the name of the template, the **show vrrp-a fail-over-policy template** command displays the contents of that template only.

show vrrp-a hostid

Description View the serial number or SoftAX UUID of all devices in the VRRP-A set.

Syntax

```
show vrrp-a hostid
```

Mode All

Example Below is an example output for this command:

```
ACOS# show vrrp-a hostid
Vrrp-a Set id is 6
  device 2              AX10A43012050032
  device 3              AX10A83012060148
ACOS#
```

Related Commands:

- hostid-append-to-vrid

show vrrp-a mac

Description Display the virtual MAC addresses of the VRIDs.

Syntax

```
show vrrp-a mac
```

Mode All

Example The following command shows the virtual MAC addresses for the default VRID (0) and VRIDs 1 and 2:

```
ACOS# show vrrp-a mac
VRRP-A vrid MACs
0          021f.a000.0020
1          021f.a000.0021
2          021f.a000.0022
```

show vrrp-a te-mac

Description View the Traffic Engineering (TE) MAC address of each VRRP VRID configured on the Multi-PU platform.

Syntax

```
show vrrp-a te-mac
```

Mode All

Usage This command is supported only on the Multi-PU platform.

Example Below is an example output for this command:

```
ACOS# show vrrp-a te-mac
VRID : 0
   Inside MAC 021f.a000.0003
   Outside MAC 021f.a010.0003
VRID : 5
   Inside MAC 021f.a000.002b
   Outside MAC 021f.a010.002b
```

show vrrp-a partition

Description View VRRP-A information for all partitions.

Syntax

```
show vrrp-a partition partition-name
```

Parameter	Description
partition-name	Show a specific partition's VRID status.

Mode All

Usage This command is only valid in the shared partition.

Example Example output for this command:

```
ACOS# show vrrp-a partition shared
Local device ID: 1
Partition    vrid  Active(P,W)     Standby(P,W)
shared       0     2 (150,65534)    1 (11,65534)
shared       13    2 (150,65534)    1 (11,65534)
```

The fields in this output are described in the following table:

Field	Description
Local device ID	Device ID of the device on which this command was executed.
Partition	Name of the partition.
vrid	VRID configured in the partition.
Active (P,W)	Device number, priority (P), and weight (W) of the active device in the VRID. For example: `2 (150,65534)` means the active device is device 2, the priority is 150, and the weight is 65534.
Standby (P,W)	Device number, priority (P), and weight (W) of the standby device in the VRID.

show vrrp-a setid-monitor

Description Display the VRRP-A set information.

Syntax

```
show vrrp-a setid-monitor
```

Mode All

Introduced in Release 2.7.0

show vrrp-a statistics

Description View VRRP-A statistics.

Syntax

```
show vrrp-a statistics
```

Mode All

Example Example output for this command:

```
ACOS-Active#show vrrp-a statistics
```

```
Session Sync Packets                    Sent      Received
-----------------------------------------------------------
Conn Sync:                               0          0
Conn Query:                              0          0
Session Sync Msg                        Sent      Received
-----------------------------------------------------------
Conn Sync Create Session:                0          0
Conn Sync Update Age:                    0          0
Conn Sync Del Session:                   0          0
Conn Sync Update Seq Num:                0          0
Conn Sync Create with Ext:               0          0
Conn Sync Update LSN RADIUS:             0          0
Conn Sync Update LSN Fullcone:           0          0
Conn Sync Update SCTP Session:           0          0
Conn Sync Create Persist Session Pkts: 0          0
Conn Sync Delete Persist Session Pkts: 0          0
Conn Sync Update Persist Age Pkts:       0          0
Conn Sync Established state Pkts:        0          0
Conn Sync Total Info Pkts:               1000       0
Conn Sync Acos Monitoring Entities:      0          0
Session Sync Send Errors
-------------------------
Conn Sync Get Buff Failure:              0
Conn Sync Get Buff Failure No Route:     0
Conn Sync Get Buff Failure Wrong Port: 0
Conn Sync Invalid Interface:       0
Conn Sync forward CPU:             0
Conn Sync query forward CPU:       0
Session Sync Send Errors
-------------------------
Conn Sync Create Conn Exists:      0
Conn Sync Del Conn not Found:      0
Conn Sync Virt Port Not Found:     0
Conn Sync Real Port Not Found:     0
Conn Sync NAT Pool Error:          0
Conn Sync Get Conn Failure:        0
Conn Sync Proc Ext Bit Failure:    0
Conn Sync App Type Invalid:        0
Conn Sync Protocol Invalid:        0
Conn Sync no SG node found:        0
```

```
Conn Sync SFW:                    0
Conn Sync Insert Tuple:           0
Conn Sync Ext PPTP:               0
Conn Sync Create Static Standby: 0
Conn Sync NAT Create Standby:     0
Conn Sync LSN Create Standby:     0
Conn Sync Ext RTSP:               0
Conn Sync Reserve HA Conn:        0
Conn Sync NAT Alloc Standby:      0
Conn Sync Seq Deltas Failure:     0
Conn Sync FTP Control Failure:    0
Conn Sync LSN ACL Failure:        0
Conn Sync Zone Failure:           0
Conn Sync LSN ACL Idle Timeout Failure: 0
Conn Sync SIP TCP ALG Failure:    0
Conn Sync H323 TCP ALG Failure:   0
Conn Sync NAT ALG TCP INFO Failure: 0
Conn Sync LSN Fullcone Failure:   0
Conn Sync NAT MAC Failure:        0
Conn Sync FW LOG Failure:         0
Conn Sync FW HTTP Logging Failure: 0
Conn Sync Length Invalid:         0
Conn Sync unexpected session sync packets: 0
Conn Sync Type Invalid:           0
Conn Sync unexpected session sync packets: 0
Conn Sync Type Invalid:           0
Conn Sync Unknown Type:           0
Conn Sync Packet Empty:           0
Conn Sync 'dst' not found for vport inline:0
Conn Sync ddos drop Failure:      0
Conn Sync invalid sync packets Failure: 0
Conn Sync bad protocoll Failure:         0
Conn Sync non-existing vgroup  Failure: 0
Conn Sync inactive peer Failure:         0

Persistent Session Sync Receive Errors:
----------------------------------------
Persist Conn Sync Length Invalid:                  0
Persist Conn Sync Get Conn Failure:                0
Persist Conn Sync Proc Ext Bit Failure:            0
```

```
Persist Conn Sync Virt Port Not Found:              0
Persist Conn Sync Real Port Not Found:              0
Persist Conn Sync Virt Port Type Invalid:           0
Persist Conn Sync Protocol Invalid:                 0
Persist Conn Sync Type Invalid:                     0
Persist Conn Sync Process Mandatory Invalid:        0
Persist Conn Sync No Service Group Found:           0
Persist Conn Sync No Service Group Info Found:      0
Session Query Send Errors:
----------------------------------------
Conn Query Get Buff Failures:                       0
Conn Query Invalid Interface:                       0
Session Query Receive Errors:
----------------------------------------
Conn Query Unknown Type:                            0
Conn Query Packet Empty:                            0
Conn Query Packet Full:                             0
aFlex Table Entry Information          Sent      Received
------------------------------------------------------------
aFlex Table Entry Add:                  0         0
aFlex Table Entry Append:               0         0
aFlex Table Entry Delete:               0         0
aFlex Table Entry Incr:                 0         0
aFlex Table Entry Lookup:               0         0
aFlex Table Entry Lifetime:             0         0
aFlex Table Entry Replace:              0         0
aFlex Table Entry Set:                  0         0
aFlex Table Entry Timeout:              0         0
aFlex Table Entry FastSync:             1000      0
aFlex Table Entry Send Error:           0
aFlex Table Entry Send Not Eligible:    0
Max Sync Msg Per Packet   Min Sync Msg Per Packet
------------------------------------------------------------
Data CPU 1           0                          0
Data CPU 2           0                          0
Max Query Msg Per Packet  Max Query Msg Per Packet
------------------------------------------------------------
Data CPU 1           0                          0
Data CPU 2           0                          0
```

show vrrp-a vrid-lead

Description View the lead VRID configuration on the system.

Syntax

```
show vrrp-a vrid-lead
```

Mode All

Example Below is an example output for this command:

```
ACOS# show vrrp-a vrid-lead
vrrp-a vrid-lead default-vrid-lead
   partition shared vrid 0
vrrp-a vrid-lead lead1
  partition shared vrid 1

ACOS(NOLICENSE)#
```

This example shows that two lead VRIDs are configured; the “default-vrid-lead” on the shared partition, and also “lead1” on the shared partition.

Scaleout

Scaleout is a solution where multiple ACOS devices form a cluster to provide the same set of services as a single infrastructure. The Scaleout technology enables CGN, Gi/SGi Firewall, and standalone Firewall services to be provided across multiple devices for load distribution and better scalability. The services provided by one or more NAT pools can be spanned across multiple devices that form a Scaleout cluster.

Scaleout supports dynamically adding or removing devices to the cluster. When the number of devices in the cluster change, the traffic gets rebalanced automatically.

This reference lists the CLI configuration and show commands that apply specifically to Scaleout.

Configuration Commands

scaleout

Description Enter Scaleout configuration mode.

Syntax

```
[no] scaleout cluster-id
```

Replace *cluster-id* with the ID of the cluster you are creating or configuring. Only one Scaleout cluster ID can be configured for one ACOS device.

Mode Configuration mode

Example Enter Scaleout configuration mode for cluster 3.

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)#
```

NOTE: Configure devices with the same scaleout cluster-id within the same scaleout cluster.

scaleout apps enable

Description Enables scaleout in CGN, Gi/SGi Firewall, or Standalone Firewall deployment.

Syntax

```
scaleout apps enable
```

Mode Scaleout configuration mode

scaleout apps separate-v4-v6-traffic-map enable

Description Enables to separate traffic maps for IPv4 and IPv6.

Syntax

```
scaleout apps separate-v4-v6-traffic-map enable
```

Default Disabled

Mode Scaleout configuration mode

Usage By default, this command is disabled and the IPv4 and IPv6 traffic-map will be the same. When it is enabled, the IPv4 and IPv6 traffic-maps will not be the same.

Example The following command enables separating the IPv4 and IPv6 traffic-maps:

```
ACOS(config)#scaleout apps separate-v4-v6-traffic-map enable
```

scaleout active-user-group-assignment

Description Activates the specified user-group-assignment template. The scaleout cluster starts forwarding packets based on the user-group assignments defined in the active template.

NOTE:
- A NAT IP must not match any assignment in the active user-group-assignment template.
- When Fixed-NAT is used with scaleout active user-group-assignment, the broadcast addresses and network addresses are not skipped in the Fixed-NAT mapping.

Syntax

```
scaleout active-user-group-assignment template
```

Mode Scaleout configuration mode

Usage Only one template can be active per partition at a time, and the active template cannot be modified.

To modify the active user-group assignment, you must copy the active template to a new template, apply the necessary modification, and then activate the new template using the **active-user-group-assignment** command.

Example The following commands activate the user-group assignment template *tp1*:

```
ACOS(config)# scaleout user-group-assignment-template tp1
ACOS(config-user-group)# 178.245.136.0/21 assignment-prefix-length 30
ACOS(config-user-group)# 188.56.224.0/20 assignment-prefix-length 29

ACOS(config)# scaleout active-user-group-assignment tp1
```

scaleout distributed-forwarding fw

Description Enables the distributed forwarding for the Firewall.

Syntax

```
scaleout distributed-forwarding fw {enable | disable |
session-offload-direction {uplink | downlink | both |
threshold {udp | tcp}}
no scaleout distributed-forwarding fw threshold
```

Parameter	Description
enable	Enables the distributed forwarding for the firewall.
disable	Disables the distributed forwarding for the firewall. This is the default option.
session-offload-direction	Configures the session offload direction. • `uplink` – Enables the session offload only in the uplink direction. • `downlink` – Enables the session offload in the downlink direction. • `Both` – Enables the session offload in both

Parameter	Description
	directions. This is the default option.
threshold	Configures the packet threshold value to offload the session. The value can be 4 – 63. The default value is 5. • `udp` – Configures the threshold for the udp session offload. • `tcp` – Configures the threshold for the tcp session offload.

Default See descriptions

Mode Scaleout configuration mode

Example The following configuration example enables the scaleout distributed forwarding for the Firewall with the session offload in the uplink direction and the threshold value set to 6.

```
ACOS(config)# scaleout distributed-forwarding fw enable
ACOS(config)# scaleout distributed-forwarding fw session-
offload-direction uplink
ACOS(config)# scaleout distributed-forwarding fw threshold 6
```

scaleout distributed-forwarding slb

Description Enables the scaleout distributed forwarding for SLB.

Syntax

```
scaleout distributed-forwarding slb {enable | disable | tcp-
threshold | udp-threshold}
```

Parameter	Description
enable	Enables the distributed forwarding for slb.
disable	Disables the distributed forwarding for slb.
tcp-threshold	Configures the threshold for the tcp session offload. The value can be 4 – 63. The default value is 5.
udp-threshold	Configures the threshold for the udp session offload. The value can be 4 – 63. The default value is 5.

Default See descriptions

Mode Scaleout configuration mode

Usage This feature reduces the number of packet redirections in SLB Scaleout which improves its packet handling performance.

Example The following configuration example enables the scaleout distributed forwarding for SLB with the threshold value set to 6 for the TCP session offload.

```
ACOS(config)# scaleout distributed-forwarding slb enable
ACOS(config)# scaleout distributed-forwarding slb tcp-
threshold 6
```

scaleout user-group-assignment-template

Description Configures a user-group assignment template that defines how the traffic is divided among user-groups based on the IP prefixes. The specified IP prefix is divided into subnets, and each subnet is sequentially assigned to a user-group.

NOTE: This command takes effect only when the template is activated using the scaleout active-user-group-assignment command.

Syntax

```
scaleout user-group-assignment-template template-name
```

Replace *template-name* with the name of the template, up to 63 characters long.

This command enters the User-Group Assignment template Configuration mode where the following commands are available:

Parameter	Description
ipv4-prefix | *ipv6-prefix*	Specify the IPv4 or IPv6 prefix that needs to be divided into user-groups. • **assignment-prefix-length** - Specify **assignment-prefix-length** to group multiple IPs into larger subnet blocks. By

Parameter	Description
	default, traffic is assigned to user-groups at the single IP level (/32). For IPv4 prefix, the default value is 32, meaning each user group is assigned a single IP address instead of a subnet. For IPv6 prefix, the default value is 128. • **`assignment-prefix-auto`** - Automatically breaks down the assignment prefix into small prefixes so that each user-group is assigned with only one subnet. It can be used with user-group-range option, in which case only the user groups within the specified range are considered.

Parameter	Description
	NOTE: - The assignment-prefix-length is calculated if the assignment-prefix-auto is configured. You can verify the calculated assignment-prefix-length using the `show scaleout user-group-assignment template` command. - The maximum number of subnets allowed is 512. - The assignment-prefix-auto will not be configured if the number of user-groups is not a power of 2. - The assignment-prefix-auto will not be configured if there is no room to allocate for all user-groups. For example, if the user-group-assignment is as below `30.30.30.0/31 assignment-prefix-auto user-group-range 0 to 3` Then there are only 2 assignments which is not enough for user-group 0 to 3. • **`private-ip`** - Sets the assignment as private, and no BGP route will be advertised for it. • **`service-config-template`** - Configures a scaleout service config template to use. This can be applied to Firewall and CGN traffic. If the service-config-template is applied to CGN traffic, the NAT pool traffic must also have the same service-config template configured. If there is a

Parameter	Description
	mismatch, the packet will be dropped. • **user-group-range** -- Configures user group range to which the prefixes are to be assigned. The default is 0 to 255. **NOTE:** On a multi-PU platform, - The number of user-groups must be even. - The IPv4 user-group-range must start with an even number and end with an odd number.

Default See descriptions

Mode Scaleout configuration mode

Usage This command configures a user-group assignment template to distribute traffic based on an IPv4 or IPv6 prefix. By default, traffic is assigned to user-groups at the single IP level (/32). However, you can use **assignment-prefix-length** to group multiple IPs into larger subnet blocks.

For example, the command **178.245.136.0/23 assignment-prefix-length 29** divides the IP prefix into /29 subnets and assigns them sequentially: 178.245.136.0/29 to User-Group 0, 178.245.136.8/29 to User-Group 1, and so on. However, if **assignment-prefix-length 29** is not specified, the system defaults to /32, assigning each individual IP to a separate user-group. In this case, 178.245.136.0/32 is assigned to User-Group 0, 178.245.136.1/32 to User-Group 1, 178.245.136.2/32 to User-Group 2, and so on.

NOTE:

- A maximum of eight templates can be configured in a system.
- IP address overlapping is forbidden between any two prefix assignments.
- If **prefix-quota-length** is set while using NAT64 or DS-Lite, the **user-group-assignment-prefix** length must be less than or equal to the **prefix-quota-length**. This ensures that all traffic within a given prefix quota is assigned to a single user group and processed by the same node in the scaleout cluster. For example, if the NAT64 **prefix-quota-length** is 96, the **user-group-assignment-prefix** can be set to any value in the range of 1 to 96.
- The system ipv6-prefix-length must be set before activating a user-group-assignment template.
- When the user-group-assignment template is configured, the IPv6 assignment-prefix-length has to match the system ipv6-prefix-length.

Example The following commands define a user-group assignment template *tp1* that splits traffic from the prefix 178.245.136.0/23 into 64 smaller /29 subnet-based user groups:

```
ACOS(config)# scaleout user-group-assignment-template tp1
ACOS(config-template:tp1)# 178.245.136.0/23 assignment-prefix-length 29
```

Example The following commands automatically breaks down the prefix:

```
ACOS(config)# scaleout user-group-assignment-templatetp1
ACOS(config-template:tp1)# 178.245.136.0/26 assignment-prefix-auto
```

Example The following commands allows assignment of prefixes to a range of user-groups (0 to 127 and 128 to 255):

```
ACOS(config)# scaleout user-group-assignment-templatetp1
ACOS(config-template:tp1)# 178.245.136.0/24 assignment-prefix-length/31 user-group-range 0 to 127
ACOS(config-template:tp1)# 178.245.136.0/24 assignment-prefix-length/31 user-group-range 128 to 255
```

cgnv6 scaleout nat-ip-hashing-scheme

Description Configure the NAT IP hashing methodology for advertising NAT IPs assigned to the user group

Syntax

```
cgnv6 scaleout nat-ip-hashing-scheme {route-aggregation | mod-user-groups}
```

Parameter	Description
route-aggregation	By default, the NAT IPs are aggregated and then allocated to a user group. The aggregated NAT IPs are advertised as a single route.
mod-user-groups	Reverts to hashing the NAT IPs and assigning to the user group that contains the inside user with the same hash value.

Mode Scaleout configuration mode

Usage By default, the NAT IP route aggregation configuration is enabled. Use **mod-user-groups** during upgrade to revert to NAT IP hashing methodology for advertising NAT IPs assigned to the user group.

cluster-devices

Description Enters Scaleout cluster configuration mode to configure devices in a cluster.

Syntax

```
cluster-devices
```

Mode Scaleout configuration mode

Example The following example shows how to enter cluster configuration mode for cluster 3:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# cluster-devices
ACOS(config-cluster:3-cluster-devices)#
```

local-device

Description Enters Scaleout local device configuration mode to configure the local device in a cluster.

Syntax

```
[no] local-device
```

Mode Scaleout configuration mode

Example The following example shows how to enter local device configuration mode for cluster 3 and set the priority of the local device:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# priority 1
ACOS(config-cluster:3-local-device)# start-delay 30
```

id

Description Assign an ID to the local device.

Syntax

```
[no] idnum
```

Replace *num* with an ID for the device.

Default No default ID is assigned.

Mode Scaleout local device configuration

Example The following example shows how to assign an ID of 4 to the local device:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# id 4
```

l2-redirect

Description Configures an interface for L2 redirection.

Syntax

```
[no] l2-redirect interface {ethernet num | trunk num} [vlan id]
```

Default None

Mode Scaleout local device configuration

Example The following example shows how to configure an L2-redirect interface with the default VLAN:

```
ACOS3(config)# scaleout 2
ACOS3(config-cluster:2)# local-device
ACOS3(config-cluster:2-local-device)# priority 230
ACOS3(config-cluster:2-local-device)# id 3
ACOS3(config-cluster:2-local-device)# l2-redirect interface
ethernet 1
ACOS3(config-cluster:2-local-device)# l2-redirect interface
ethernet 1 vlan 2000
```

priority

Description Assigns a priority to the local device.

Syntax

```
[no] priority num
```

Replace *num* with an ID for the device.

Default No default priority is assigned

Mode Scaleout local device configuration

Example The following example shows how to assign a priority of 150 to the local device:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# priority 150
```

failure-domain

Description Configures failure-domain on the node.

Syntax

```
[no] failure-domain id-string
```

Field	Description
id-string	The name of the failure-domain.

Mode Scaleout local device configuration

Usage The failure-domain can be configured on nodes in the cluster. The nodes with the same name belong to the same failure-domain. If it is not configured, the node uses the Scaleout device-id as the failure-domain. After modifying the failure-domain, the Scaleout must be enabled.

Limitation The failure-domain is configurable only from the shared partition. The Scaleout on the node must be disabled before changing the failure-domain configuration. Else, the command will not be accepted.

Example The following commands configure failure-domain on a node:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# priority 150
ACOS(config-cluster:3-local-device)# failure-domain domain100
ACOS(config)# scaleout apps enable
```

session-sync

Description Configures a session synchronization interface that is used to handle session synchronization requests.

Syntax

```
[no] session-sync
```

Default None.

Mode Scaleout local device configuration

Example The following example shows how to configure a session sync interface:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# session-sync
```

start-delay

Description Configures the time the scaleout must wait to join the cluster after the device boot up. The value can be 10 to 300.

Syntax

```
start-delay num
```

Mode Scaleout local device configuration

Example The following command shows how to configure the time the scaleout must wait to join the cluster after the device boot up:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# start-delay 12
```

tracking-template

Description Configures a failover template that can be associated to a Scaleout cluster to track events such as the operational state of BGP peers, routes, gateways, interfaces, trunks, and VLANs.

Syntax

```
[no] tracking-template [multi-template <name> | template
<name> [ipv4 | ipv6]]
```

Parameter	Description
`multi-template <name>`	Configures multi-tracking template to be used by Scaleout.
`template <name>`	Configures tracking template to be used by Scaleout. • `ipv4` - Only affects the traffic map for the default IPv4 Traffic map and any IPv4 Traffic Slices' Traffic Maps for the specific partition. • `ipv6` - Only affects the traffic map for the default IPv6 Traffic map for the specific partition.

Default None

Mode Scaleout local device configuration

Example The following example shows how to configure a failover template for IPv4 traffic:

```
ACOS(config)# scaleout 1
ACOS(config-cluster:1)# local-device
ACOS(config-cluster:1-local-device)# tracking-template
ACOS(config-cluster:1-local-device-tracking-template)#
template temp ipv4
```

```
ACOS(config-cluster:1-local-device-tracking-template-template)
#threshold 100 down
```

Example

In the following example, 3 tracking templates are defined in the partition.
Template ‘all-cases’ is the default tracking template that affects all IPv4/IPv6 traffic. The IPv4 tracking template ‘bgp-ipv4’ affects all IPv4 traffic and the IPv6 tracking template ‘bgp-ipv6’ affects all IPv6 traffic:

```
ACOS(config)#resource-track all-cases
ACOS(config-resource-track:all-cases)#interface ethernet1
weight 100

ACOS(config)#resource-track bgp-ipv4
ACOS(config-resource-track: bgp-ipv4)#bgp 2.2.2.2 weight 50

ACOS(config)#resource-track bgp-ipv6
ACOS(config-resource-track: bgp-ipv6)#bgp 3001::1 weight 50

ACOS(config)#scaleout 1
ACOS(config-cluster:1)#local-device
ACOS(config-cluster:1-local-device)#template all-cases
ACOS(config-cluster:1-local-device-template all-
cases)#threshold 100 down
ACOS(config-cluster:1-local-device)#template bgp-ipv4 ipv4
ACOS(config-cluster:1-local-device-template bgp-ipv4
ipv4)#threshold 50 down
ACOS(config-cluster:1-local-device)#template bgp-ipv6 ipv6
ACOS(config-cluster:1-local-device-template bgp-ipv6
ipv6)#threshold 50 down
```

traffic-redirection

Description

Provides options to configure redirect interfaces and determine the reachability options for redirection.

Syntax

```
[no] traffic-redirection
```

This command enters the traffic redirection configuration mode where the following commands are available:

Parameter	Description
encap	The encapsulation options to redirect the traffic. • **vxlan** - Uses vxlan for encapsulation. ○ **use-v4-vxlan** - Forces to always use IPv4 VxLAN for traffic redirection.
interfaces	The interfaces to redirect the traffic. • **ethernet** – Uses the ethernet interface for traffic redirection. • **loopback** – Uses the loopback interface for traffic redirection. The loopback interface number can be 0-10. • **trunk** – Uses the trunk interface for traffic redirection. The trunk interface number can be 1-4096. • **ve** – Uses the virtual ethernet interface for traffic redirection. The virtual ethernet interface number can be 2-4094.
reachability-options	Options to determine the reachability options for redirection. • **skip-default-route** – The default route must not be selected for redirection.

Default None

Mode Scaleout local device configuration

Usage The IPv4 traffic redirection takes place over IPv4 VxLAN tunnel and the IPv6 traffic redirection takes place over IPv6 VxLAN tunnel. Due to this, there will be a redirection failure during an upgrade from an older releases to 5.2.1-P7 and later releases. This command will force all redirections to happen over IPv4 VxLAN tunnels.

Example The following example shows how to configure traffic redirection and to make use of the IPv4 VxLAN for traffic redirection:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# local-device
ACOS(config-cluster:3-local-device)# traffic-redirection
ACOS(config-cluster:3-local-device-traff...)# encap vxlan
ACOS(config-cluster:3-local-device-traff...)# use-v4-vxlan
```

service-config

Description Configures the Scaleout templates for SLB, CGN, and VRRP.

Syntax

```
[no] service-config
```

Mode Scaleout configuration mode

Example The following example shows how to configure a Scaleout template:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)# service-config
ACOS(config-cluster:3-service-config)# template cgn
```

user-group-count

Description Configures the number of user groups for the Scaleout template.

Syntax

```
[no] user-group-count num
```

Replace *num* with a number of user groups. It can be 1 - 256. The user-group-count must be a power of 2 value starting from 1, 2, 4, … 256.

Mode Scaleout template configuration mode

Example The following example configures 32 user groups for the Scaleout template:

```
ACOS(config)# scaleout 3
ACOS(config-cluster:3)#service-config
ACOS(config-cluster:3-service-config)#template core
ACOS(config-cluster:3-service-config-tem....)#user-group-count
32
```

NOTE: When the user-group count at per partition or within a traffic slice is changed, you must clear all sessions or reboot cluster on bucket count or device group change.

match scaleout

Description Configures a match command that matches the state of the scaleout node. This may be used to permit or deny routes based on the scaleout status.

Syntax

```
[no] route-map name permit seq num
match scaleout cluster-id [ipv4 | ipv6] {up | down}
```

Parameter	Description
`match scaleout cluster-id`	Specify the cluster-ID to match the Scaleout cluster node state. • `up` – Scaleout is up (for both ipv4 and ipv6) and running. • `down` – Scaleout is down for either ipv4 or ipv6 or Scaleout is disabled. Furthermore, you can match the ipv4/ipv6 specific state based on the relevant tracking templates: • `ipv4` – matched when the state of the IPv4 tracking template goes up/down or the default tracking template goes up/down. • `ipv6` – matched when the state of the IPv6 tracking template goes up/down or the default tracking template goes up/down.

Mode Configuration mode

Example The following example shows how to configure **`route-map`** command for a node belonging to Scaleout cluster 1. The permit command is executed when the node's operational state changes to the 'down' state:

```
ACOS(config)# route-map map1
ACOS(config)# route-map map1 permit 1
ACOS(config)# route-map map1 permit 1
ACOS(config-route-map:1)# match scaleout 1 down
ACOS(config-route-map:1)# end
```

Show Commands

show cgnv6 scaleout

Description Displays IP to user group mapping information. It also displays information about the active node and the standby node.

Syntax

```
show cgnv6 scaleout
[address-mapping{inside-user address | nat-address address |
nat-pool name | fixed-nat fixed-nat-index}]
```

Parameter	Description
address-mapping	Displays IP to user group mapping information. • *inside-user* - Displays inside user to user group mapping information. • *nat-address* - Displays NAT IP to user group mapping information. • *nat-pool* - Displays user group mapping information for all NAT IPs in a NAT pool. • *fixed-nat* - Displays user group mapping information for Fixed-NAT IPs by Fixed-NAT config Index. Fixed-NAT config Index for a particular configuration can be obtained using the `show cgnv6 fixed-nat detail` command.

Usage All

Mode Configuration mode

Example The following example shows sample output for **show cgnv6 scaleout address-mapping inside-user**.

```
ACOS(config)# show cgnv6 scaleout address-mapping inside-user
1.1.1.1
```

show scaleout

Description View Scaleout information.

Syntax

```
show scaleout [all | ipv4 | ipv6]
```

Parameter	Description
all	Displays the status of both IPv4 and IPv6 Scaleout nodes.
ipv4	Displays the Scaleout member nodes for IPv4.
ipv6	Displays the Scaleout member nodes for IPv6.

Usage All

Example The following example shows sample output for the **show scaleout** command:

```
ACOS# show scaleout

Device Role : Cluster Master
Cluster Mode : Layer-3

Device 1 - Active
Device 2 - Active (Local) (Master)
Device 3 - Active
```

NOTE: If Scaleout is not configured or the connection between the nodes is lost, then a message “Scaleout is not Active” appears.

The following table describes the fields in this output:

Field	Description
Role	Shows the role of the local device (the device on which you are executing the **show scaleout** command. • When Scaleout is not configured or is inactive, a message “Scaleout is not Active” is displayed. • During Scaleout initialization and election, the node has the “Unknown Node” role. • Once the cluster master is elected, the Master node has the “Cluster Master” role, while other nodes in the cluster have the “Service Node” role. • If Scaleout gets into an inactive state, the message "Scaleout is not Active" is displayed.
Cluster Mode	Displays the cluster-mode enabled on each Scaleout cluster node at the partition level for traffic redirection and session synchronization. The cluster-mode can be one of the following: • Layer-2 (default) • Layer-3 The Layer-2 and Layer-3 mode are mutually exclusive.
Device	Shows a list of devices in the cluster. The device marked with “(Local)” is the local device; the device from which you are running the **show scaleout** command.

Example

The following example shows sample output for `show scaleout` when the following is configured:

```
Layer-2 Cluster Mode
Layer-2 redirection is configured as “l2-redirect interface
trunk 1 vlan 99”:

ACOS# show scaleout
Device Role : Cluster Master
Cluster Mode : Layer-2
```

```
Device 1 - Active
Device 2 - Active (Local) (Master)

L2-Redirection:
Status: Valid
L2 Trunk: 1
vlan: 99
```

This output shows the status of the dedicated redirect interface, the trunk and VLAN number configured for this interface.

```
Layer-3 Cluster Mode

ACOS# show scaleout
Device Role : Cluster Master
Cluster Mode : Layer-3

Device 1 - Active
Device 2 - Active (Local) (Master)
```

Example The following example shows sample output for **show scaleout** when the minimum nodes number is less than the active nodes:

```
ACOS#  show scaleout
Role - Service Node
Minimum active nodes required are 7, currently at 3

Device 1 - Waiting (Local)
Device 2 - Waiting
Device 5 - Waiting (Master)
```

Example The following example shows sample output for **show scaleout** when the minimum nodes number is reached:

```
ACOS#  show scaleout
Role - Service Node

Device 1 - Active (Master)
Device 2 - Active
Device 3 - Active (Local)
```

Example

The following is the sample output of the `show counters so-counters` command to view the counters for shadow sessions:

```
ACOS# show counters so-counters
Total packets processed for an established connection
  1781177146
Total packets redirected for an established connection
  16322633089
Total packets dropped
  0
Total packet errors
  0
Total packets in-coming
  0
Total packets processed for a new connection
  3069035747
Total packets redirected for a new connection
  25608431948
Total packets sent out
  0
Total packets redirected
  0
Total connection sync failures
  0
Total NAT reserve failures
  0
Total NAT release failures
  0
Total L7 connection syncs
  0
Total L4 connection syncs
  0
Total NAT connection syncs
  625699165
Total Xparent FW connection syncs
  604
Total redirect conns aged out
  0
```

```
Traffic MAP Not Found Drop
  31
Scaleout Not Active Drop
  31572657
Destination MAC Mistmatch Drop
  7137181
L2redirect Intf is not UP
  0
Redirect Table Error
  0
MAC Address zero Drop
  6
L3 Redirect encap error Drop
  0
L3 Redirect inner mac zero Drop
  0
L3 Redirect Decap VLAN Sanity Drop
  0
L3 Redirect Inner ipv4 fragmentation, punt slowpath
  0
L3 Redirect Inner ipv6 fragmentation, punt slowpath
  0
Total number of L3 Redirected packets received
  0
L3 Redirect received non ipv4 VXLAN packet
  0
L3 Redirect decap Rx encap params error Drop
  0
L3 Redirect Table error Drop
  0
Recevied l3 redirect packets in L2 mode Drop
  0
L3 redirect encap DF bit set
  0
L3 redirect encap Fragmentation error
  0
L3 redirect encap Internal buffer allocation error
  0
```

```
L3 redirect Table no redirect entry found error
  0
L3 Redirect Follow Shared Table error Drop
  0
L3 Redirect Invalid Device direction
  0
L3 Redirect Chassis Destination Mac Error
  0
FW internal rule update Error
  0
L3 Redirect ipv4 packet after encap more than max jumbo size
  0
L3 Redirect ipv6 packet after encap more than max jumbo size
  0
Received L3 Redirected fragmented packets too large
  0
Sent Sync message for FW Shadow session creation
  0
FW Shadow Session created
  0
Sync FW Shadow extension creation/updation
  0
Sync Shadow session stats from shadow to active
  0
Sent Sync message for FW Shadow session deletion
  0
```

Example The following example shows sample output for the Scaleout member nodes for IPv4:

```
ACOS(config)#show scaleout ipv4
Device Role  : Cluster Master
Cluster Mode : Layer-3

Device 1 - Active (Local) (Master)
Device 2 - Active
Device 3 - Active
Device 4 - Active
```

show scaleout failure-domain

Description Displays a list of all nodes and the failure-domain information.

Syntax

```
show scaleout failure-domain
```

Example The following example shows sample output for the **show scaleout failure-domain** command:

```
ACOS#show scaleout failure-domain
Failure-domain in the current cluster:
Dev-ID  |      Domain Name
---------------------------------
1     |      Default
2     |      domain100
3     |      domain200
4     |      domain200
```

The following table describes the fields in this output:

Field	Description
Dev-ID	Shows a list of device-IDs.
Domain	The name of the failure-domain. The device marked with “Default” indicates that the failure-domain is not configured and it is always unique in the cluster.

Example The following example shows sample output for the **show scaleout failure-domain** command if all nodes in the cluster belong to the same failure-domain, where Scaleout enters fallback mode:

```
ACOS(config)#show scaleout failure-domain

Failure-domain in the current cluster:

Dev-ID  |      Domain Name
---------------------------------
1       |      domain100
2       |      domain100
```

```
Fallback: [Yes]
```

show scaleout session-sync

Description View Scaleout session synchronization information.

Syntax

```
show scaleout session-sync
```

Usage All

Example The following example shows the sample output for **show scaleout session-sync**:

```
ACOS# show scaleout session-sync
Active interfaces:
None

Destination IPs:
Device Id    IPv4              IPv6
1            20.20.20.130      5000::130
```

show scaleout statistics

Description View Scaleout statistics information.

Syntax

```
show scaleout statistics
```

Usage All

Example The following example shows sample output for **show scaleout statistics**

```
ACOS# show scaleout statistics
Packets received                                1404490
Redirect packets sent                           1336905
Packets dropped                                 1
Redirected packets received                     0
FW shadow sessions created                     0
SLB shadow sessions created                     0
Traffic map not found drop                      0
SLB redirect conns aged out                     0
```

```
Scaleout not active drop                          0
SLB NAT reserve failures                          0
SLB NAT release failures                          0
Destination MAC mismatch drop                     1
L2 Redirection error dest mac zero drop           0
L2 Redirect intf not UP                           0
L2 Invalid redirect info                          0
L3 Redirect TX encap error drop                   0
L3 Redirect TX inner mac zero drop                0
L3 Redirect RX decap VLAN sanity drop             0
L3 Redirect RX non-ipv4 VXLAN packet drop         0
L3 Redirect RX decap header drop                  0
L3 Invalid redirect info                          0
L3 Redirect packet RX in L2 mode drop             0
L3 Redirect TX encap Fragmentation error          0
L3 Redirect TX no valid path entry found          0
L3 Redirect invalid device direction              0
L3 Redirect RX multi-slot Destination MAC error   0
L3 Redirect TX ipv4 Jumbo Fragmentation drop      0
L3 Redirect TX ipv6 Jumbo Fragmentation drop      0
L3 Redirect RX fragment packet too large drop     0
FW shadow session create                          0
FW shadow session delete                          0
SLB shadow session create                          0
SLB shadow session delete                          0
```

The following table describes the show scaleout statistics counters:

Field	Description
Packets received	The total data packets received by the scaleout logic. This counter will not increment for control packets (ZK health checks, packets destined to vThunder interfaces or ports, BGP/OSPF, and so on.)
Redirect packets sent	The total data packets redirected out of the node. This counter will only increment for data traffic.
Packets dropped	The total data packets dropped.

Field	Description
Redirected packets received	The total redirected data packets received on node.
FW shadow sessions created	The FW shadow sessions created.
SLB shadow sessions created	The SLB shadow sessions created.
Traffic map not found drop	The number of packets received on the node and dropped as a traffic map is not present at that time. This might happen while the cluster is reconverging.
SLB redirect conns aged out	The number of ADC L4 sessions deleted from the node as the node is neither active nor standy for the corresponsing user group and the current node is not the NAT owner of the client IP. This will typically increment after a state transition for the nodes in the cluster (node added, removed and so on).
Scaleout not active drop	The number of packets received by the cluster and dropped as Scaleout is not active on the local device. Drop is to prevent the allocation of NAT resources in non-scaleout mode, which the device may not own.
SLB NAT reserve failure	The number of times the ADC standby node failed to reserve the NAT port.
SLB NAT release failures	The number of times the ADC standy node failed to free the allocated NAT port.
Destination MAC mismatch drop	The number of packets received by the cluster and dropped as the destination MAC does not match with the receiving interface. This happens for incoming traffic packets or L2 redirected packets.
L2 redirection	The packets dropped since the destination mac

Field	Description
error dest mac zero drop	type does not match the interface type.
L2 redirect intf not UP	The number of times L2 redirect is attempted when the L2 redirect interface is configured but the interface is not working for some reason. Redirection will not be done using the configured interface but via the default L2 forwarding of the device.
L2 Invalid redirect info	The number of redirect table error due to invalid redirect information.
L3 Redirect TX encap error drop	The packets dropped due to errors during encapsulation.
L3 Redirect TX inner mac zero drop	The packets dropped since the inner destination mac address of the L3 redirected packet is zero.
L3 Redirect RX decap VLAN sanity drop	The packets dropped after decapsulation since VLAN sanity checks failed.
L3 Redirect RX non-ipv4 VXLAN packet drop	The number of packets dropped due to non-IPV4 VXLAN packets received.
L3 Redirect RX decap header drop	The number of packets dropped while decapsulating as the metadata in the VXLAN header is wrong.
L3 Invalid redirect info	The packets dropped due to L3 redirect table error before encapsulation.
L3 Redirect packet RX in L2 mode drop	The packets dropped due to the VXLAN packets received in scaleout L2 mode.
L3 Redirect TX encap Fragmentation	The packets dropped since error occurred while trying to fragment the packet.

Field	Description
Error	
L3 Redirect TX no valid path entry found	The packets dropped since no matching entries were found.
L3 Redirect invalid device direction	The packets dropped since the device direction is INVALID.
L3 Redirect RX multi-slot Destination Mac error	The packets dropped since the destination mac type does not match the interface type.
L3 Redirect TX ipv4 Jumbo Fragmentation drop	The packets dropped since it is a IPv4 jumbo packet and needs fragmentation.
L3 Redirect TX ipv6 Jumbo Fragmentation drop	The packets dropped since it is a IPv6 jumbo packet and needs fragmentation.
L3 Redirect RX fragment packet too large drop	The packets dropped since the packets are large and need fragmentation.
FW shadow session create	The sync message sent for FW shadow session creation.
FW shadow session delete	The sync message sent for FW shadow session deletion.
SLB shadow session create	The sync message sent for SLB shadow session creation.
SLB shadow session delete	The sync message sent for SLB shadow session deletion.

The following table shows the mapping of old counters to new counters:

Old Output	New Output
Pkts in	Packets received
Pkts in (conn)	Removed
Pkts in (no conn)	Removed
Pkts Redirect	Redirectpackets sent
Pkts Redirected (conn)	Removed
Pkts Redirected (no conn)	Removed
Pkts out	Removed
Pkts Dropped	Packets dropped
Pkts Errors	Removed
Conn Sync failures	Removed
	Redirected packets received
	FW shadow sessions created
NAT Reserve failures	SLB NAT reserve failures
NAT Release failures	SLB NAT release failures
L7 Sync events	Removed
L4 Sync events	Removed
NAT Sync events	Removed
FW Sync events	Removed
Redirect Conns aged out	SLB redirect conns aged out
Traffic MAP Not Found Drop	Traffic map not found drop
Scaleout Not Active Drop	Scaleout not active drop
Destination MAC Mismatch Drop	Destination MAC mismatch drop
L2 redirect intf not UP	L2 Redirect intf not UP
L2 Redirect Table Error	L2 Invalid redirect info
Destination MAC zero Drop	L2 Redirection error dest mac zero drop

Old Output	New Output
L3 Redirect encap error Drop	L3 Redirect TX encap error drop
L3 Redirect inner mac zero Drop	L3 Redirect TX inner mac zero drop
L3 Redirect Decap VLAN Sanity Drop	L3 Redirect RX decap VLAN sanity drop
L3 Redirect Inner ipv4 fragmentation	Removed
L3 Redirect Inner ipv6 fragmentation	Removed
L3 Redirected packets in	Removed (NOTE: merged with “Redirected packets received”)
L3 Redirect recv non-ipv4 VXLAN packet	L3 Redirect RX non-ipv4 VXLAN packet drop
L3 Redirect decap header Drop	L3 Redirect RX decap header drop
L3 Redirect Table Error	L3 Invalid redirect info
L3 Redirect Follow Shared Table Error	Removed (NOTE: merged with “L3 Invalid redirect info”)
L3 Redirect packet rcvd in L2 mode Drop	L3 Redirect packet RX in L2 mode drop
L3 Redirect encap DF bit set	Removed
L3 Redirect encap Fragmentation Error	L3 Redirect TX encap Fragmentation error
L3 Redirect encap Internal Buff Alloc Error	Removed
L3 Redirect Table No Entry Found	L3 Redirect TX no valid path entry found
L3 Redirect Invalid Device Direction	L3 Redirect invalid device direction
L3 Redirect Chassis	L3 Redirect RX multi-slot Destination

Old Output	New Output
Destination Mac Error	MAC error
FW Internal Rule Update Error	Removed (NOTE: Added as a log)
L3 Redirect ip Jumbo Fragmentation Drop	L3 Redirect TX ipv4 Jumbo Fragmentation drop
L3 Redirect ipv6 Jumbo Fragmentation Drop	L3 Redirect TX ipv6 Jumbo Fragmentation drop
L3 Redirect Fragment packet too large Drop	L3 Redirect RX fragment packet too large drop

The following are the newly added counters:

- Packets received
- Redirect packets sent
- Redirected packets received
- FW shadow sessions created
- FW shadow session create
- FW shadow session delete
- SLB shadow sessions created
- SLB shadow session create
- SLB shadow session delete

The following are the counters that are removed:

- Pkts in (conn)
- Pkts in (no conn)
- Pkts Redirected (conn)
- Pkts Redirected (no conn)
- Pkts out
- Pkts Error
- Conn Sync failures

- L7 Sync events
- L4 Sync events
- NAT Sync events
- FW Sync events
- L3 Redirect Inner ipv4 fragmentation
- L3 Redirect Inner ipv6 fragmentation
- L3 Redirect encap DF bit set
- L3 Redirect encap Internal Buff Alloc Error

The following table shows the counters that are renamed:

Old Counter Names	New Counter Names
Redirect Conns aged out	SLB redirect conns aged out
Destination MAC zero drop	L2 redirection error dest mac zero drop
L2 Redirect Table Error	L2 Invalid redirect info
L3 Redirect encap error Drop	L3 Redirect TX encap error drop
L3 Redirect inner mac zero Drop	L3 Redirect TX inner mac zero drop
L3 Redirect Decap VLAN Sanity Drop	L3 Redirect RX decap VLAN sanity drop
L3 Redirect recv non-ipv4 VXLAN packet	L3 Redirect RX non-ipv4 VXLAN packet drop
L3 Redirect decap header Drop	L3 Redirect RX decap header Drop
L3 Redirect Table Error	L3 Invalid redirect info
L3 Redirect packet rcvd in L2 mode Drop	L3 Redirect packet RX in L2 mode Drop
L3 Redirect encap Fragmentation Error	L3 Redirect TX encap Fragmentation Error
L3 Redirect Table No Entry Found	L3 Redirect TX no valid path entry found

Old Counter Names	New Counter Names
L3 Redirect Invalid Device Direction	L3 Redirect TX Invalid Device Direction
L3 Redirect Chassis Destination Mac Error	L3 Redirect RX multi-slot Destination MAC Error
L3 Redirect ip Jumbo Fragmentation Drop	L3 Redirect TX ipv4 Jumbo Fragmentation Drop
L3 Redirect ipv6 Jumbo Fragmentation Drop	L3 Redirect TX ipv6 Jumbo Fragmentation Drop
L3 Redirect Fragment packet too large Drop	L3 Redirect RX Fragment packet too large Drop

show scaleout traffic-map

Description View Scaleout traffic-map information.

Syntax

```
show scaleout traffic-map [all | ipv4 | ipv6 | service-config-template <temp-name>]
```

Parameter	Description
`all`	Displays the default IPv4 Traffic Map and all service config template Traffic Maps along with the default IPv6 Traffic Map.
`ipv4`	Displays the traffic map for IPv4 traffic.
`ipv6`	Displays the traffic map for IPv6 traffic.
`service-config-template <temp-name>`	Specify the traffic map for the specified service-config template.

Usage All

Example The following example shows the sample output for **`show scaleout traffic-map`**:

```
ACOS# show scaleout traffic-map
```

```
User-Group  Active Device   Standby Device   New Act Device
New Stby Device
0           1               2                -
-
1           1               2                -
-
2           1               2                -
-
3           1               2                -
-
4           2               1                -
-
5           1               2                -
-
6           1               2                -
-
7           2               1                -
-
8           1               2                -
-
9           2               1                -
-
10          1               2                -
-
11          2               1                -
-
12          1               2                -
-
13          1               2                -
-
14          1               2                -
-
```

If CGN Scaleout is not configured or inactive, the sample output of the **show scaleout traffic-map** command is as follows:

```
ACOS# show scaleout traffic-map
User-Group  Active Device   Standby Device   New Act Device
New Stby Device
               -
```

Example The following example shows the sample output for **`show scaleout traffic-map ipv4`**:

```
Number of Traffic Map Tables: 3
Default shared
User-group Number of Traffic Map Tables: 256
User-Group Active Device Standby Device New Act Device New
Stby Dev
0           1               2               -
-
1           1               2               -
-
2           1               2               -
-
3           1               2               -
-
4           1               2               -
-
5           1               2               -
-
-
-
255         4               3               -
-

service type : traffic-slice 2
User-group Number of Traffic Map Tables: 2
User-Group  Active Device   Standby Device   New Act Device
New Stby Device
0            3                4                -
   -
1            4                3                -
   -

service type : traffic-slice 4
User-group Number of Traffic Map Tables: 4
User-Group  Active Device   Standby Device   New Act Device
New Stby Device
0            1                2                -
   -
```

```
1               3                   4                   -
    -
2               4                   3                   -
    -
3               2                   4                   -
    -
```

Example The following example shows the sample output for **`show scaleout traffic-map ipv6`**:

```
Number of Traffic Map Tables: 1
Default-IPv6 shared
User-group Number of Traffic Map Tables: 256
User-Group Active Device Standby Device New Act Device New
Stby Dev
0            1               2                   -
-
1            1               2                   -
-
2            1               2                   -
-
3            1               2                   -
-
4            1               2                   -
-
5            1               2                   -
-
-
-
255          4               3                   -
-
```

show scaleout traffic-redirection

Description View Scaleout traffic redirection information.

Syntax **`show scaleout traffic-redirection`**

Usage All

Example The following example shows the sample output for **show scaleout traffic-redirection:**

```
ACOS# show scaleout traffic-redirection
Configured Interface IPs advertised:
None
Destination IPs:
Device Id       Direction       IP
2               CGN Inside      123.123.123.1
2               CGN Outside     30.30.30.2
2               FW Inside       123.123.123.1
2               FW Outside      30.30.30.2

Destination IPv6s:
Device Id       Direction       IP
2               CGN Inside      5000::130
2               FW Inside       5000::130
```

show scaleout user-group-assignment inside-user <IPv4 | IPv6>

Description Shows inside user to user-group mapping.

NOTE: The command can be used for both Firewall and CGN deployment.

Syntax

```
show scaleout user-group-assignment inside-user  IPv4 Inside User | IPv6 Inside User
```

Usage All

Example The following example shows the sample output for **show scaleout user-group-assignment inside-user IPv4 Inside User** command:

```
ACOS# show scaleout user-group-assignment inside-user
178.245.136.9
User Group: 4, Active-Node: 2, Standby-Node: 1, Application:
Firewall, Service-Template: GLOBAL
```

The following table describes the fields in the command output.

Field	Description
User Group	The number of user groups.
Active-Node	The number of active nodes.
Standy-Node	The number of standby nodes.
Application	The application running.
Service-Template	The name of the service template.

show scaleout user-group-assignment template

Description View user-group assignment information for a specified user-group assignment template. This show command output provides an overview of how traffic is distributed among user-groups based on the IP prefixes.

NOTE: The command can be used for both Firewall and CGN deployment.

Syntax `show scaleout user-group-assignment template` *template_name*

Usage All

Example The following example shows the sample output for **`show scaleout user-group-assignment template`** command:

```
ACOS# show scaleout user-group-assignment template tp1
178.245.136.0/21:
  assignment-prefix-length      32
  Number of prefixes:          256
  Number of IP in each prefix:   8
  Prefixes per user-group:       1
  User group range start:        0
  User group range end:        255
188.56.224.0/20:
  assignment-prefix-length      32
  Number of prefixes:          512
  Number of IP in each prefix:   8
  Prefixes per user-group:       2
  User group range start:        0
  User group range end:        255
```

The following table describes the fields in the command output.

Field	Description
Assignment-prefix-length	The number assignment prefix length created for the specified IP prefix.
Number of prefixes	The number subnet divisions created for the specified IP prefix.
Number of IP in each prefix	The number of IP addresses in each subnet division.
Prefixes per user-group	The number of subnet divisions per user-group.
User group range start	The first user-group index in the assignment range.
User group range end	The last user-group index in the assignment range.

Carrier-Grade NAT

Thunder Carrier-Grade NAT (CGN), the most advanced carrier-grade networking solution, provides high-performance CGNAT with protocol translation that allows service providers and enterprise to extend IPv4 investment while simultaneously transitioning to IPv6 standards.

This reference lists the CLI configuration and show commands that apply specifically to CGN.

Configuration Commands

Large Scale NAT

class-list (for LSN)

Description Configure an IP class list for use with Large Scale NAT (LSN).

Prerequisite Configure the LSN LIDs or Fixed-NAT LIDs before configuring the class list entries.

Syntax `[no] class-list {list-name} [file | ipv4 [file] | ipv6 [file]]`

Parameter	Description
list-name	Adds the list to the running-config.
file	Saves the list to a file.
ipv4 | ipv6	Specifies the class-list type as IPv4 or IPv6.

This command changes the CLI to the configuration level for the specified class list, where the following command is available.

NOTE: The other configuration commands at this level are not applicable to LSN.

Command	Description
[**no**] *priv-addr*/*mask-length* {**glid** *num* | **lid** *num* | **lsn-lid** *num* | **lsn-radius-profile** *num*}	Specifies the internal clients. The priv-addr option specifies the internal host or subnet address. The /mask-length specifies the network mask or mask length. • The **glid***num* option specifies an global LSN LID to apply to matching clients. • The **lid***num* option specifies a non-LSN LID to apply to matching clients. • The **lsn-lid***num* option specifies an LSN LID to apply to matching clients. • The **lsn-radius-profile** *num* option specifies an LSN RADIUS Profile Index to apply to matching clients.

Default None

Mode Configuration mode

Usage As an alternative to configuring class entries on the ACOS device, you can configure the class list using a text editor on another device, then import the class list onto the ACOS device.

For more information, see “Large Scale NAT” topic in the IPv4-to-IPv6 Transition Solutions Guide.

Example The following commands configure a class list to bind internal subnet 5.5.5.x/24 to LSN LID 5:

```
ACOS(config)# class-list list1
ACOS(config-class list)# 5.5.5.0 lsn-lid 5
```

cgnv6 enable-port-batch-v1

Description Enable Port Batching v1.

Syntax `[no] cgnv6 enable-port-batch-v1`

Default None

Mode Configuration mode

Usage If no pre-existing port-batch-v1 configurations are detected, use this command to enable Port Batching v1 manually, prior to configuring port-batching size, port-overloading, and NAT Pool configurations.

cgnv6 ecmp 4-tuple-hash

Description Enable ECMP route and link load balancing to support 4-tuple hashing based on Source IP, Source Port, Destination IP, and Destination Port.

Syntax `[no] cgnv6 ecmp 4-tuple-hash`

Mode Configuration mode

Usage This feature is enhanced to support 4-tuple hashing for UDP/TCP/ICMP for Static-NAT and LW-4o6 technologies, in addition to the previously supported UDP/TCP for DSLite, LSN, Fixed-NAT, NAT64, and Gi/SGi-FW transparent sessions.

Example The following shows how to enable ECMP 4-tuple hashing:.

```
ACOS(config)# cgnv6 ecmp 4-tuple-hash
```

cgnv6 global domain-list

Description Configure the parameters for the CGNv6 domain-list at a global level.

Syntax `[no] cgnv6 global domain-list [ interval minutes | fail-interval seconds | aaaa-query { enable | disable } ]`

Parameter	Description
interval *<minutes>*	Specify the global query interval (in minutes) for DNS resolution. You can specify a value in the range 1-1440 minutes. The ACOS device sends DNS queries (A and

Parameter	Description
	AAAA type) to the DNS server for resolution. The query interval is the time between DNS queries if the previous query is successful. Each domain in the domain-list has a default value for the query interval. However, there is no pre-defined or default setting for the query interval at the global level. You need to explicitly define this value so that it is applied globally across all domains.
fail- interval *<seconds>*	Specify the global fail-interval (in seconds) for DNS resolution. You can specify a value in the range 3-600 seconds. The fail-interval is the time in seconds that ACOS waits to restart the next DNS query process for a domain since the last failure. A DNS query process includes a maximum of 5 retry queries sent (for both A and AAAA records) at an interval of 3 seconds if the previous query failed. Each domain in the domain-list has a default value for the fail-interval. However, there is no pre-defined or default setting for the fail-interval at the global level. You need to explicitly define this value so that it is applied globally across all domains.
aaaa-query { **enable** | **disable** }	Enable or disable the DNS AAAA query record for each domain in the CGNv6 domain-list. When this command is disabled, ACOS does not send an AAAA query record for the domain under the CGNv6 domain-list. This implies that only A query records are sent

Parameter	Description
	for DNS resolution. This command is enabled by default.

Default NA

Mode Configuration mode

NOTE: This global configuration is only effective for domains with default parameters. This implies that if you configure the query interval and fail-interval at the domain level (using the domain-list command), the configuration at the global level will not take effect.

Example The following command sets the global query interval to 2 minutes:

```
ACOS(config)# cgnv6 global domain-list interval 2
```

Example The following command sets the global fail-interval to 20 seconds:

```
ACOS(config)# cgnv6 global domain-list fail-interval 20
```

Example The following command disables the AAAA query record for each domain in the CGNv6 domain list:

```
ACOS(config)# cgnv6 global domain-list aaaa-query disable
```

Related Commands:

- domain-list

cgnv6 logging

Description Configures a severity level for NAT pool exhaustion log messages.

Syntax

```
[no] cgnv6 logging {nat-quota-exceeded | nat-resource-exhausted} level {critical | notice | warning | pool-based-log {cycle}}
```

Parameter	Description
nat-quota-exceeded	Configures the warning level of error messages when the NAT pool quota is exceeded. The following options

Parameter	Description
	are available: • **critical** configures error messages to be flagged as critical. • **notice** configures error messages to be flagged as notifications. • **warning** configures error messages to be flagged as warnings.
nat-resource-exhausted	Configures the warning level of error messages when the NAT pool resources are exhausted. The following options are available” • **critical** configures error messages to be flagged as critical. • **notice** configures error messages to be flagged as notifications. • **warning** configures error messages to be flagged as warnings.
pool-based-log	Configures the frequency of logs when pool-based logs such as NAT pool resources are exhausted. The pool-based log cycle works for logging by the control CPU only. The following option is available: • **cycle** - Configures error messages every 1 to 1800 seconds. If this parameter is not configured, the default value, 30, is automatically applied. The `cgnv6 logging pool-based log cycle 0` returns to the original logging behavior, where logs are generated per data CPU every 30 seconds. This is only available in the shared partition. Once enabled, this applies to all NAT pools in all

Parameter	Description
	shared and L3V partitions. The logs for L3V partitions are logged in their respective partitions.

Default By default all resource exhaustion error messages are flagged as "Critical," and all quota exceeded error messages are flagged as "Warning."

Mode Configuration Mode

Usage Use these command to configure a severity level for NAT pool exhaustion messages. The following log messages fall into each category:

Resource Exhausted:

- LOG_MSG_A10LB_LSN_NAT_PORT_UNAVAILABLE
- LOG_MSG_A10LB_LSN_NEW_USER_RESOURCE_UNAVAILABLE
- LOG_MSG_A10LB_LST_IP_ALL_PORT_EXHAUSTED
- LOG_MSG_A10LB_LSN_USER_QUOTa_CREATION_FAILED
- LOG_MSG_A10LB_LSN_FULLCONE_CREATE_FAILED
- LOG_MSG_A10LB_NAT_121_POOL_STAT_ADDR_EXHAUSTED
- LOG_MSG_A10LB_FIXED_NAT_PORT_UNAVAILABLE_EXCESS
- LOG_MSG_A10LB_FIXED_NAT_PORT_UNAVAILABLE_ONE_USER
- LOG_MSG_A10LB_FIXED_NAT_PORT_UNAVAILABLE_EXCESS_NO_IPLIST

Quota Exceeded:

- LOG_MSG_A10LB_LSN_NAT_PORT_UNAVAILABLE
- LOG_MSG_A10LB_LSN_NEW_USER_RESOURCE_UNAVAILABLE
- LOG_MSG_A10LB_LSN_IP_ALL_PORT_EXHAUSTED
- LOG_MSG_A10LB_LSN_USER_QUOTA_CREATION_FAILED
- LOG_MSG_A10LB_LSN_FULLCONE_CREATION_FAILED
- LOG_MSG_A10LB_NAT_121_POOL_STAT_ADDR_EXHAUSTED
- LOG_MSG_A10LB_FIXED_NAT_PORT_UNAVAILABLE_EXCESS
- LOG_MSG_A10LB_FIXED_NAT_PORT_UNAVAILABLE_ONE_USER

- LOG_MSG_A10LB_FIXED_NAT_PORT_UNAVAILABLE_EXCESS_NO_IPLIST
- LOG_MSG_A10LB_FIXED_NAT_QUOTA_EXCEEDED_EXCESS
- LOG_MSG_A10LB_FIXED_NAT_QUOTA_EXCEEDED_ONE_USER
- LOG_MSG_A10LB_FIXED_NAT_QUOTA_EXCEEDED_EXCESS_NO_IPLIST

All *_ONE_USER errors extend to _TWO_USER, _THREE_USER, _FOUR_USER, etc.

The `pool-based-log` command is effective for the following types of logs:

Log Types Supported	Attributes
USER_QUOTA_ICMP_EXCEEDED	Session exceeding logs
USER_QUOTA_UDP_EXCEEDED	
USER_QUOTA_TCP_EXCEEDED	
USER_QUOTA_ESP_EXCEEDED	
EXT_USER_QUOTA_UDP_EXCEEDED	
EXT_USER_QUOTA_TCP_EXCEEDED	
SESSION_QUOTA_EXCEEDED	
NEW_USER_RESOURCE_UNAVAILABLE	Resource Unavailable Logs
ICMP_NAT_PORT_UNAVAILABLE	Nat Port Unavailable Logs
UDP_NAT_PORT_UNAVAILABLE	
TCP_NAT_PORT_UNAVAILABLE	
FULLCONE_CREATION_FAILED	Creation Failed Logs
USER_QUOTA_CREATION_FAILED	

cgnv6 lsn alg

Description Disables or re-enables Application Level Gateway (ALG) support for LSN and Fixed-NAT.

Syntax

```
[no] cgnv6 lsn alg
{dns |esp | ftp | h323 | mgcp | pptp | rtp-stun-timeout | rtsp
```

```
| sip | tftp}
{enable | disable}
```

Parameter	Description
dns	Disables ALG support for Domain Name System (DNS).
esp	Enables or disables ALG support for Encapsulating Security Payload (ESP).
ftp	Enables or disables ALG support for File Transfer Protocol (FTP).
h323	Enables or disables ALG support H323 standard.
mgcp	Enables or disables ALG support for Media Gateway Control Protocol (MGCP).
pptp	Enables or disables ALG support for Point-to-Point Tunneling Protocol (PPTP).
rtp-stun-timeout	Changes the RTP/RTCP Session Traversal Utilities for NAT (STUN) timeout for the RTP/RTCP sessions created by SIP, MGCP, and H323. The timeout duration is 2 to 10 minutes. The default timeout value is 5 minutes.
rtsp	Enables or disables ALG support for Real Time Streaming Protocol (RTSP).
sip	Enables or disables ALG support for Session Initiation Protocol (SIP).
tftp	Enables or disables ALG support for Trivial File Transfer Protocol (TFTP).

Default ALG support for FTP is enabled by default. ALG support for the other protocols is disabled by default.

Mode Configuration mode

cgnv6 lsn alg sip rtp-stun-timeout

Description Change the RTP/RTCP Session Traversal Utilities for NAT (STUN) timeout for full-cone sessions.

Syntax

```
[no] cgnv6 lsn alg sip rtp-stun-timeout minutes
```

Replace *minutes* with the timeout duration (2-10 minutes)

Default 5

Mode Configuration mode

cgnv6 lsn attempt-port-preservation

Description Enable LSN port preservation. Port preservation attempts to use the same source protocol port for a client's public address (NAT address) that is used in the client's inside address.

Syntax

```
[no] cgnv6 lsn attempt-port-preservation {disable | enable}
```

Default Enabled

Mode Configuration mode

Usage Even when port preservation is disabled, it is possible in rare cases for the same protocol port to be used.

cgnv6 lsn endpoint-independent-filtering

Description Configure endpoint-independent filtering.

Syntax

```
[no] cgnv6 lsn endpoint-independent-filtering
{tcp | udp}
```

Parameter	Description
tcp | udp	Specifies the Layer 4 protocol. If you want to apply the command to both TCP and UDP, enter the command twice, specifying a different protocol each time. The following options are available: • **port** configures a single destination port or Port Range Start • **session-limit** limits the number of EIF sessions that can be created per port.

Default Disabled

Mode Configuration mode

Usage Ensure that both EIF and EIM are enabled for a destination port or a port range. If EIF is enabled for a port where EIM is disabled or vice versa, the EIM filtering will fail when packets are dropped.

NOTE: When IP stateful firewall is configured, EIF configuration should only be done for the inside L4 ports. In these cases, the inside L4 ports should be configured as the destination ports since traffic is originating from outside.

cgnv6 lsn endpoint-independent-mapping

Description Configure endpoint-independent mapping for both ephemeral and well-known ports.

Syntax

```
[no] cgnv6 lsn endpoint-independent-mapping
{tcp | udp}
```

Parameter	Description
`tcp | udp`	Specifies the Layer 4 protocol. If you want to apply the command to both TCP and UDP, enter the command twice, specifying a different protocol each time.

Default Disabled

Mode Configuration mode

Usage Ensure that both EIF and EIM are enabled for a destination port or a port range. If EIF is enabled for a port where EIM is disabled or vice versa, the EIM filtering will fail when packets are dropped.

cgnv6 lsn enhanced-user-tracking

Description Configures the enhanced user tracking for viewing the peak session utilization, NAT port utilization, and aggregated upstream and downstream byte and packet count per subscriber for both LSN and NAT64.

The enhanced user tracking log must be configured at the partition level.

Before configuring the enhanced user tracking log, the following logs can be configured to include session byte count, LSN subscriber information, and radius attributes in the `enhanced-user-tracking` log:

```
ACOS(config)# cgnv6 template logging template_name
ACOS(config-logging:template_name)# include-session-byte-count
ACOS(config-logging:template_name)# log user-data
ACOS(config-logging:template_name)# include-radius-attribute
user-data
```

Syntax `[no] cgnv6 lsn enhanced-user-tracking`

Default Disabled

Mode Configuration mode

Usage The information in the enhanced user tracking log can be used to detect anomaly attack in the client's network. The log information also provides enhanced visibility for allocating user quota values for sessions and ports. When there are new NAT IPs, the NAT port utilization log helps to allocate the NAT IPs to the appropriate NAT pools for efficient utilization.

cgnv6 lsn hairpinning

Description Configure filtering for hairpinning.

Syntax

```
[no] cgnv6 lsn hairpinning
{filter-none | filter-self-ip | filter-self-ip-port}
```

Parameter	Description
filter-none	Allows for self-hairpinning for UDP packets only. This is the default behavior for UDP packets.
filter-self-ip	Drops packets that have the same inside client IP address for both the source and destination.
filter-self-ip-port	Drops packets that have the same inside client IP address and protocol port number for both the source and destination. This option may be needed if double NAT is used.

- **filter-none** - UDP

- **filter-self-ip port** - TCP

Mode Configuration mode

cgnv6 lsn half-close-timeout

Description Configure the TCP half-closed session timeout for LSN.

Syntax

```
[no] cgnv6 lsn half-close-timeout seconds
```

Replace *seconds* with the timeout (2-3000 seconds).

Default No default timeout is set.

Mode Configuration mode

Usage The LSN TCP half-closed timeout is separate from the TCP idle-timeout.

cgnv6 lsn health-check-gateway

Description Configure enforcement of gateway health monitoring prior to redistributing LSN NAT pool prefixes.

Syntax

```
[no] cgnv6 lsn health-check-gateway ip-addr
```

Replace *ip-addr* with the IPv4 or IPv6 address for the gateway for enforcement.

Default Disabled.

Mode Configuration mode

Usage If any of the specified gateways fail a health check, the ACOS device will discontinue advertising LSN NAT pool prefixes during route redistributions. This command needs to be entered again for each gateway.

cgnv6 lsn icmp

Description Send ICMP Destination Unreachable messages when there are no protocol ports available for NAT mappings, or when a a user quota is exceeded.

Syntax

```
[no] cgnv6 lsn icmp
{send-on-port-unavailable |
```

```
send-on-user-quota-exceeded}
{
admin-filtered |
disable |
host-unreachable
}
```

Parameter	Description
send-on-port-unavailable	Sends ICMP Destination Unreachable message when there are no protocol ports available for NAT mappings.
send-on-user-quota-exceeded	Sends ICMP Destination Unreachable message when a a user quota is exceeded.
admin-filtered	Sends code type 3, code 13, administratively filtered.
disable	Disable ICMP Unreachable messages for the specified event.
host-unreachable	Sends code type 3, code 1 for IPv4, and type 1 code 3 for IPv6.

Default The default for **send-on-port-unavailable** is **disable**. The default for **send-on-user-quota-exceeded** is **admin-filtered**.

Mode Configuration mode

cgnv6 lsn inbound-refresh

Description Enable or disable the session aging time for NAT translation.

Syntax

```
[no] cgnv6 lsn inbound-refresh {disable | enable}
```

Default Enabled

Mode Configuration mode

Usage This command disables or enables resetting of the age-out time for NAT translation when inbound packets are received. This command does not apply for outbound packets.

cgnv6 lsn inbound-refresh-full-cone

Description Enable or disable the session aging time for LSN full-cone sessions.

Syntax `cgnv6 lsn inbound-refresh-full-cone {disable | enable}`

Default Enabled

Mode Configuration mode.

Usage When this command is disabled, inbound packets that match an existing data session are allowed. However, if the packets match a firewall full-cone session, new session will be created by the active full-cone session but rejected by the inactive full cone session and session's age will not be refreshed.

cgnv6 lsn inside source class-list

Description Bind an IP class list for use with LSN.

Syntax `[no] cgnv6 lsn inside source class-list list-name`

Replace *list-name* with the name of the class list.

Default None

Mode Configuration mode

Usage The class list must already be configured. You can import the class list or configure it on the ACOS device. For more information, see “Large Scale NAT” topic in the IPv4-to-IPv6 Transition Solutions Guide.

cgnv6 lsn ip-selection

Description Specify the method for LSN to use to select IP addresses within a pool.

Syntax `[no] cgnv6 lsn ip-selection method`

Replace *method* with one of the following:

- **random** – Selects addresses randomly, instead of using any of the other methods.
- **round-robin** – Selects addresses sequentially.
- **least-used-strict** – Selects the address with the fewest NAT ports of any type (TCP or UDP) used. This option is not applicable to ICMP.

- **least-udp-used-strict** – Selects the address with the fewest UDP NAT ports used.
- **least-tcp-used-strict** – Selects the address with the fewest TCP NAT ports used.
- **least-reserved-strict** – Selects the address with the fewest TCP or UDP NAT ports reserved.
- **least-tcp-reserved-strict** – Selects the address with the fewest TCP NAT ports reserved.
- **least-udp-reserved-strict** – Selects the address with the fewest UDP NAT ports reserved.
- **least-users-strict** – Selects the address with the fewest users.

Default **random**

Mode Configuration mode

Usage The IP address selection method applies only to the IP addresses within individual pools. The method does not apply to selection of pools within a pool group. LSN randomly selects a pool from within a pool group, then uses the configured IP address selection method to select an address from within the pool.

cgnv6 lsn logging default-template

Description Set a configured LSN traffic logging template as the default template for all LSN pools.

Syntax

```
[no] cgnv6 lsn logging default-template template-name
```

Replace *template-name* with the name of the LSN traffic logging template to use as the default for all LSN pools.

Default Not set

Mode Configuration mode

Usage The NAT logging template you plan to use as the default must already be configured.

You also can assign a NAT logging template to an individual pool. In this case, the NAT logging template assigned to the pool is used instead of the default NAT logging template.

Example The following commands configure a NAT logging template, then set it as the default logging template for LSN:

```
ACOS(config)# cgnv6 server syslog1 192.168.1.100
ACOS(config-real server)# port 514 udp
ACOS(config-real server)# exit
ACOS(config)# cgnv6 service-group syslog udp
ACOS(config-cgnv6 svc group)# member syslog1:514
ACOS(config-cgnv6 svc group)# exit
ACOS(config)# cgnv6 template logging lsn_logging
ACOS(config-logging:lsn_logging)# log port-mappings creation
ACOS(config-logging:lsn_logging)# service-group syslog
ACOS(config-logging:lsn_logging)# exit
ACOS(config)# cgnv6 lsn logging default-template lsn_logging
```

Related Commands:

- cgnv6 lsn logging pool

cgnv6 lsn logging partition

Description Assigns a separate VRF/L3V instance for the CGN logging servers and to enable system logs to be routed from different partitions.

Syntax

```
[no] cgnv6 lsn logging partition
```

Parameter	Description
shared	Selects the shared partition.
Name	Selects the partition name for logging.

Default Not set.

Mode Configuration mode

NOTE: From a L3V partition, any other partition can also be referenced. From a shared partition, only allowed L3V partition can be referenced.

cgnv6 lsn logging pool

Description Assign a NAT logging template to an LSN pool.

Syntax

```
[no] cgnv6 lsn logging pool pool-name template template-name
```

Parameter	Description
pool-name	Specifies the LSN pool.
template-name	Specifies the NAT logging template.

Default Not set. If a NAT logging template has been set as the default NAT logging template, that template is used.

Mode Configuration mode

Usage The NAT logging template you plan to use must already be configured.

cgnv6 lsn port-batching

Description Enable port batching. Port batching reduces logging by allocating a set of multiple ports to the client at the same time, and generating only a single log message for the batch of ports.

Syntax

```
[no] cgnv6 lsn port-batching size
{1 | 8 | 16 | 32 | 64 | 128 | 256 | 512}
```

Specifies the number of ports to allocate in each batch.

Default Disabled

Mode Configuration mode

NOTE: New users must explicitly use the cgnv6 enable-port-batch-v1 command to enable Port Batching v1 manually, prior to configuring this command.

cgnv6 lsn port-batching tcp-time-wait-interval

Description Configure the timeout interval before TCP NAT ports can be reused after they have been released.

Syntax

```
[no] cgnv6 lsn port-batching tcp-time-wait-interval num
```

Specifies the timeout of TCP ports in minutes. You can specify a value between 0-10 minutes.

Default 2 minutes

Mode Configuration mode

Example The following example configures CGNv6 LSN port batching, with a TCP timeout interval of 5 minutes before TCP ports in a batch can be reused after they are released.

```
ACOS(config)# cgnv6 lsn port-batching tcp-time-wait-interval 5
```

cgnv6 lsn port-overloading

Description Enable or disable Port Overloading.

Syntax

```
[no] cgnv6 lsn port-overloading
{tcp | udp}
```

Parameter	Description
tcp | **udp**	Enable or disable port overloading behavior for TCP or UDP traffic specifically.
port-num [**to** *port-num*]	Enables port overloading for the specified protocol and port or port range.

Default Port overloading is enabled for all ports, 1-65535.

Usage Configuration mode

cgnv6 lsn port-overloading allow-different-user

Description Allows an overloaded port to be used by more than one client.

Syntax

```
[no] cgnv6 lsn port-overloading allow-different-user
```

Default By default, a port can be overloaded to create multiple mappings only for the same client.

Mode Configuration mode

cgnv6 lsn port-overloading unique

Description Change the granularity for Port Overloading.

Syntax

```
[no] cgnv6 lsn port-overloading unique
{destination-address |
destination-address-and-port}
```

Parameter	Description
destination-address	The granularity is based on destination IP address.
destination-address-and-port	The granularity is based on destination IP address and destination protocol port.

Default **destination-address-and-port**

Mode Configuration mode

cgnv6 lsn port-reservation

Description Configure static LSN mappings for a range of protocol ports for an internal address.

Syntax

```
[no] cgnv6 lsn port-reservation
inside priv-ipaddr start-priv-portnum end-priv-portnum
nat public-ipaddr start-public-portnum end-public-portnum
```

Parameter	Description
priv-ipaddr	Specifies the internal IP address.
start-priv-portnum	Specifies the beginning (lowest-numbered) protocol port number in the range of internal protocol port numbers.
end-priv-portnum	Specifies the ending (highest-numbered) protocol port number in the range of internal protocol port numbers.
public-ipaddr	Specifies the public IP address to map to the internal IP address.
start-public-	Specifies the beginning public protocol port number in the range to map to the internal protocol port

Parameter	Description
portnum	numbers.
end-public-portnum	Specifies the ending public protocol port number in the range to map to the internal protocol port numbers.

Default None. If LSN is configured, LSN mappings are created and deleted dynamically.

Mode Configuration mode

cgnv6 lsn strictly-sticky-nat

Description Configure to strictly adhere to the sticky NAT behaviour, regardless of configuring destination IP addresses in the LSN rule-list.

Syntax

```
[no] cgnv6 lsn strictly-sticky-nat
```

Default None.

Mode Configuration mode.

Usage Use this command to strictly adhere to the sticky NAT behavior. Regardless of configuring destination IP addresses in the LSN rule-list configuration, ACOS uses the same mapping for all traffic between the client and the NAT IP addresses once the mapping is dynamically assigned.

cgnv6 lsn stun-timeout

Description Configure the LSN STUN timeout. The LSN STUN timeout specifies how long a NAT mapping for a full-cone session is maintained after the data session ends.

Syntax

```
[no] cgnv6 lsn stun-timeout {tcp | udp}
port port-num [to port-num] minutes
```

Parameter	Description
tcp | **udp**	Specifies the Layer 4 protocol. If you omit this option, the command applies to both TCP and

Parameter	Description
	UDP.
port *port-num* [**to** *port-num*]	Specifies an individual port or a custom port range.
minutes	Specifies the timeout, 0-60 minutes.

Default 2, for all TCP and UDP ports (1-65535)

Mode Configuration mode

Usage If you do not use the **ephemeral**, **well-known**, or **port** option, the command applies to ports 1-65535.

cgnv6 lsn syn-timeout

Description Configure the SYN timeout for LSN.

Default [**no**] **cgnv6 lsn syn-timeout** *seconds*

Replace *seconds* with the timeout (2-30 seconds).

Default 4

Mode Configuration mode

Usage The LSN SYN timeout is separate from the IP NAT translation timeout.

cgnv6 lsn tcp mss-clamp

Description Configure TCP maximum segment size (MSS) clamping. MSS clamping checks the TCP MSS value in packets from IPv4 clients and, if necessary, changes it before sending the NATted request to the server.

Syntax **[no] cgnv6 lsn tcp mss-clamp** {**none** | **fixed** *n* | **subtract** *s* [**min** *n*]}

Parameter	Description
none	Does not change the MSS value.
fixed *n*	Changes the MSS to the length you specify.
subtract *s*	Reduces the MSS if it is longer than the specified

Parameter	Description
[**min** *n*]	number of bytes. This option sets the MSS based on the following calculations: • If MSS minus S is greater than N, subtract S from the MSS. • If MSS minus S is less than or equal to N, set the MSS to N. The subtract method of MSS clamping is used by default, with the following values: S = 40 bytes N = 416 bytes Using these values, the default MSS clamping calculations are as follows: • If MSS minus 40 is greater than 416, subtract 40 from the MSS. • If MSS minus 40 is less than or equal to 416, set the MSS to 416.

Default The **none** option is used by default.

Mode Configuration mode

cgnv6 lsn tcp reset-on-error

Description Send TCP resets to LSN clients in response to invalid TCP packets from the inside network.

Syntax `[no] cgnv6 lsn tcp reset-on-error outbound disable`

Default Enabled

Mode Configuration mode

cgnv6 lsn-lid

Description Configures a limit ID (LID) for LSN.

NOTE: Some LSN LID commands apply only to other features, and are described in the topics for those features.

Syntax

```
[no] cgnv6 lsn-lidnum
```

Replace *num* with the LSN LID number, 1-1023.

This command changes the CLI to the configuration level for the specified LSN LID, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to LSN.

Command	Description
[no] conn-rate-limit *num*	The maximum number of connections a client can attempt to initiate per second. The value can range from 1-65535.
[no] ds-lite inside-src-permit-list *list-name*	For Dual-stack Lite (DS-Lite), uses a class list to specify the hosts or subnets that are permitted to be NATted. Any IPv4 addresses that do not match the class list are not NATted.
[no] extended-user-quota {**tcp** | **udp**} **service-port** *portnum* **sessions** *num*	Configures a per-user extended quota for essential services. The port option specifies the Layer 4 protocol port of the service, and can be 1-65535. The sessions option specifies how many extended sessions are allowed for the protocol port, and can be 1-255.
[no] lsn-rule-list destination *list-name*	Matches traffic based on destination IP address, traffic type, or protocol port, in addition to matching on the source IP addresses in the class list that uses this LID. If traffic matches both a source IP address in the class list and a destination address, traffic type, or protocol port in the rule list, the action specified in the rule list is applied to the traffic.

Command	Description
[no] **name** *string*	Assigns a name to the LID.
[no] **override** {**none** | **drop** | **pass-through**}	Overrides NAT for matching traffic, and performs the specified action instead: • **none** – Applies source NAT if configured (default). • **drop** – Drops the traffic. • **pass-through** – Forwards the traffic without performing NAT.
[no] **respond-to-user-mac**	Enables MAC-based nexthop routing. When MAC-based nexthop routing is enabled, the ACOS device sends the reply to an inside client's request back through the same route hop on which the request was received. The ACOS device identifies the route hop based on its MAC address. The ACOS device sends the reply to the MAC address, instead of using the route table to select the next hop for the reply.
[no] **source-nat-pool** *pool-name*	Binds an LSN NAT pool to the LID.
[no] **user-quota** {**tcp** | **udp** | **icmp** | **session**| **session-tcp**| **session-udp**} *quota-num* [**reserve** *reserve-num*]	Configures the per-user mapping quota for the specified protocol such as tcp, udp, icmp. The quota-num option specifies the maximum number of sessions allowed per client and can be 1-64000. The **reserve** option allows you to specify how many ports to reserve on a NAT IP for each user, 0-64000. If unspecified, a warning message: "Warning: Applying the configured value to 'reserve' as the default setting." is displayed. **NOTE:** The `reserve` can be configured only for user-quota tcp and user-quota udp.

Command	Description
	Configures user quota based on sessions: • `session` - Configures user quota for the number of data sessions. It can be 1-2147483647. • `session-tcp` - Configures user quota for the number of TCP sessions. It can be 1-2147483647. • `session-udp` - Configures user quota for the number of UDP sessions. It can be 1-2147483647.
[no] user-quota-prefix-length *length-num*	Configures the NAT64 user quota prefix length <1-128>.

Default The LSN LID options have the following default values:

- **ds-lite** – not set
- **extended-user-quota** – not set
- **lsn-access-list** – not set
- **name** – not set
- **override** – not set
- **respond-to-user-mac** – disabled
- **source-nat-pool** – not set
- **user-quota** {**tcp** | **udp** | **icmp**} – Not set. By default, the reserve value is the same as the user-quota value.
- **user-quota sessions** – not set
- **user-quota sessions-tcp** – not set
- **user-quota sessions-udp** – not set
- **user-quota-prefix-length** – Uses the global NAT64 configured value

Mode Configuration mode

Example The following commands configure an LSN LID. The LID is bound to pool "LSN_POOL1". Per-user quotas are configured for TCP, UDP, and ICMP.

For UDP, this class of users will reserve only 100 UDP ports instead of 300. An extended quota of sessions per client is allocated for TCP port 25 (SMTP).

```
ACOS(config)# cgnv6 lsn-lid 5
ACOS(config-lsn lid)# source-nat-pool LSN_POOL1
ACOS(config-lsn lid)# user-quota tcp 100
ACOS(config-lsn lid)# user-quota udp 300 reserve 100
ACOS(config-lsn lid)# user-quota icmp 10
ACOS(config-lsn lid)# extended-user-quota tcp service-port 25
sessions 3
```

Example The following commands configure an LSN LID in which MAC-based nexthop routing is enabled:

```
ACOS(config)# cgnv6 lsn-lid 1
ACOS(config-lsn lid)# respond-to-user-mac
ACOS(config-lsn lid)# exit
```

Example The following commands configure a class list that maps inside clients to the LSN LID:

```
ACOS(config)# class-list mac-reply-clients
ACOS(config-class list)# 192.168.0.0 /16 lsn-lid 1
```

Example The following commands configure user-quota session-tcp and user-quota session-udp as 512 in an LSN LID:

```
ACOS(config)# cgnv6 lsn-lid 1
ACOS(config-lsn lid)# source-nat-pool p1
ACOS(config-lsn lid)# user-quota session-tcp 512
ACOS(config-lsn lid)# user-quota session-udp 512
```

Example The following commands configure the user-quota tcp with reserve in an LSN LID:

```
ACOS(config)# cgnv6 lsn-lid 1
ACOS(config-lsn lid)# user-quota tcp 5000 reserve 5000
ACOS(config-lsn lid)#
```

Example The following commands display the error message if reserve is not configured with user-quota tcp or udp:

```
ACOS(config)# cgnv6 lsn-lid 1
```

```
ACOS(config-lsn lid)# user-quota tcp 5000
Configuration accepted. Applying the configured value to quota
'reserve' as the default setting.
```

Related Commands:

- cgnv6 nat icmp always-source-nat-errors

cgnv6 lsn-radius-profile

Description Configure a RADIUS profile that assigns clients to LSN LIDs based on the value of the custom attribute from the RADIUS server.

Syntax

```
[no] cgnv6 lsn-radius-profile num
```

This command changes the CLI to the configuration level for the specified RADIUS server profile, where the following command is available.

NOTE: The other configuration commands at this level are not applicable to LSN.

Parameter	Description
radius {**default** | *attribute-type*} [**exact-value** *string* | **starts-with** *string*] **lsn-lid** *num*	Matches on the attribute values from the RADIUS server, and specifies the LSN LID to use for handling clients that have the matching attribute value. The *attribute-type* can be one of the following: • **default** – Matches on clients who do not have any of the following custom attributes. • **msisdn** – Matches on client MSIDSN. • **imei** – Matches on client IMEI. • **imsi** – Matches on client IMSI. • **custom1** – A10-CGN-Radius-Custom-1 • **custom2** – A10-CGN-Radius-Custom-2 • **custom3** – A10-CGN-Radius-Custom-3

Parameter	Description
	To specify match criteria, use one of the following options: • **exact-value** *string* – Matches only on an exact attribute value. • **starts-with** *string* – Matches on only the beginning portion of an attribute value. The **lsn-lid** option specifies the LSN LID to use for handling clients that have the matching attribute value.

Default Not set

Mode Configuration mode

cgnv6 lsn-rule-list

Description Configure an LSN rule list. You can add an LSN rule list to an LSN LID to specify the actions to perform on matching traffic. This command changes the CLI to the configuration level for the specified rule list.

NOTE: You also can use LSN rule lists for NAT64 and DS-Lite.

Syntax

```
[no] cgnv6 lsn-rule-list list-name
```

Replace *list-name* with the name of the rule list.

Command	Description
[no] default	Enters the configuration level for the default set of rules. The default set of rules is used for traffic that does not exactly match an IP host or subnet rule. • **[no]dscp[any** | *dscp-value*]**action set-dscp** {**inbound***dscp-value* [**outbound***dscp-value*] | **outbound***dscp-value* [**inbound***dscp-value*]} • **[no] icmp** {**action** *action* | **no-action**}

Command	Description
	◦ **dnat ipv4-list** *list-name* {**action** *action* | **no-action**} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **others** {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no** *action* | **no-action**} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **tcp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no-snat** | **port-list** *num*} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]}

Command	Description
	◦ **snat pool** {*pool-name* | *pool-group-name*} ◦ **template http-alg** *template-name*
[**no**] **default**	• [**no**] **udp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no-snat** | **port-list** *num*} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*}
[no] **domain-ip**	Specifies Domain IP for LSN Rule-List. • **sampling-enable** {**all** | **hits**} Enables baselining for all requests or for requests that match the destination rule.
[**no**] **domain-list-name** *string*	Enters the configuration level for the set of rules to apply to the specified domain list name. • [**no**]**dscp**[**any** | *dscp-value*]**action set-dscp** {**inbound***dscp-value* [**outbound***dscp-value*] | **outbound***dscp-value* [**inbound***dscp-value*]} • [**no**] **icmp** {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through**

Command	Description
	◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **others** {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **tcp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no-snat** | **port-list** *num*} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} ◦ **template http-alg** *template-name*
[**no**] **domain-list-name** *string*	• [**no**] **udp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no-snat** | **port-list** *num*}

Command	Description
	◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*}
[**no**] **domain-name** *string*	Enters the configuration level for the set of rules to apply to the specified domain name. • [**no**]**dscp**[**any** | *dscp-value*]**action set-dscp** {**inbound***dscp-value* [**outbound***dscp-value*] | **outbound***dscp-value* [**inbound***dscp-value*]} • [**no**] **icmp** {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **others** {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]}

Command	Description
	◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **tcp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no-snat** | **port-list** *num*} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*} ◦ **template http-alg** *template-name*
[**no**] **domain-name** *string*	• [**no**] **udp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} ◦ **dnat ipv4-list** *list-name* {**no-snat** | **port-list** *num*} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} ◦ **snat pool** {*pool-name* | *pool-group-name*}
[**no**] **http-match-domain-name**	Enables matching domain name in the HTTP request.
[**no**] **ip** *ipv4addr* **/***mask-*	Enters the configuration level for the set of rules to apply to the specified IP host address or subnet.

Command	Description
length	• **[no] dscp** {{**any** | *dscp-value*}**action set-dscp** {**inbound** *dscp-value* | **outbound** *dscp-value*}} • **[no] default** {**action** *action* | **no-action**} Replace *action* with the following options: ○ **dnat** {**domain** *domain-name* | **ipv4-list** *list-name*} ○ **drop** ○ **one-to-one-snat** {**pool** *pool-name*} ○ **pass-through** ○ **set-dscp** { **inbound** *dscp-value* | **outbound** *dscp-value*} ○ **snat {pool** [*pool-name* | *pool-group-name*]**}** • **[no] icmp** {**action** *action* | **no-action**} Replace *action* with the following options: ○ **dnat {domain** *domain-name* | **ipv4-list** *list-name***}** ○ **drop** ○ **one-to-one-snat {pool** *pool-name***}** ○ **pass-through** ○ **set-dscp** {**inbound** *dscp-value* | **outbound** *dscp-value* } ○ **snat {pool** [*pool-name* | *pool-group-name*]**}** • **[no] others {action** *action* | **no-action}** Replace *action* with the following options: ○ **dnat {domain** *domain-name* | **ipv4-list** *list-name***}** ○ **drop**

Command	Description
	◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* | **outbound** *dscp-value* } ◦ **snat pool** {*pool-name* | *pool-group-name*} • [**no**] **tcp { port** {**0** | *portnum* { [**to** *portnum*] | **action** *action* | **no-action**}} } Replace *action* with the following options: ◦ **dnat {domain** *domain-name* | **ipv4-list** *list-name* {**no-snat** {**vrid** *vrid* } | **port-list** *port-list-name* {**no-snat** {**vrid** *vrid*}}} ◦ **drop** ◦ **one-to-one-snat pool** *pool-name* ◦ **pass-through** ◦ **set-dscp** {**inbound** *dscp-value* | **outbound** *dscp-value* } ◦ **snat pool** {*pool-name* | *pool-group-name*} ◦ **idle-timeout** {*num* | *fast*} ◦ **template http-alg** *template-name*
[**no**] **ip** *ipv4addr* **/***mask-length*	• [**no**] **udp{port**{0 |*portnum* { [**to** *portnum*] | **action** *action* | **no-action** }}} Replace *action* with the following options: ◦ **dnat {domain** *domain-name* | **ipv4-list** *list-name* {**no-snat** {**vrid***vrid*} | **port-list** *port-list-name* {**no-snat** {**vrid** *vrid*}}} ◦ **drop** ◦ **one-to-one-snat** {**pool** *pool-name*}

Command	Description
	○ **pass-through** ○ **set-dscp** {**inbound** *dscp-value* **| outbound** *dscp-value* } ○ **idle-timeout** {*num* | **fast**} ○ **snat pool** {*pool-name* | *pool-group-name*}

The following commands are available at this level:

- [**no**] **dscp** [**any** | *dscp-value*] **action set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} – Matches based on the DSCP classification in traffic, and marks the DSCP value before forwarding the traffic.
- **default** {**action** *action* | **no-action**}- Specifies the default action for matching all the traffic.
- [**no**] **icmp** {**action** *action* | **no-action**} – Specifies the action for matching ICMP traffic.
- [**no**] **others** {**action** *action* | **no-action**} – Specifies the action for matching traffic that is not ICMP, TCP, or UDP traffic.
- [**no**] **tcp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} – Specifies the action for matching TCP traffic.
- [**no**] **udp port** {**0** | *portnum* [**to** *portnum*]} {**action** *action* | **no-action**} – Specifies the action for matching UDP traffic.

The *action* can be one of the following:

- **dnat** {**domain** *domain-name <1-63>* | **ipv4-list** *list-name <1-63>* **{no-snat {vrid** *vrid}<1-31>* **| port-list** *port-list-name <1-128>* {**no-snat** {**vrid** *vrid<1-31>*}}} – Applies destination NAT action using domain-name or IP list.
- **drop** – Drops the traffic.
- **idle-timeout** {*num <2-129600>*| **fast**}– Configures an idle-timeout or fast aging for the traffic on the configured destination network or host.

- **one-to-one-snat** {**pool** *pool-name <1-63>*} – Applies one-to-one source NAT.
- **pass-through** – Forwards the traffic without performing NAT.
- **set-dscp** {**inbound** *dscp-value* [**outbound** *dscp-value*] | **outbound** *dscp-value* [**inbound** *dscp-value*]} – Performs DSCP marking.
- **snat** {**pool** [*pool-name<1-63>* | *pool-group-name <1-63>]*} – Performs NAT using the specified pool or pool group. This option can be used to redirect the traffic to use a different pool or pool group than the one in the LID definition.
- **template** {**http-alg** *template-name<1-63>*} – Processes traffic based on the specified HTTP-ALG template.

NOTE: The **dnat domain** option is applicable only to NAT44 and NAT64 translations.

The **pass-through** option is not applicable to NAT64 or DS-Lite. For these features, the option is ignored and the traffic is processed based only on source IP address. (No rule list is applied.)

The **no-action** option excludes matching traffic from the actions in the rule list, but still performs NAT for the traffic. (For more information, see IPv4-to-IPv6 Transition Solutions Guide.)

Default None

Mode Configuration mode

Usage After you configure the rule list, you can add it to an LSN LID.

For NAT64, the traffic matching and action are applied to IPv4 addresses after conversion from IPv6 to IPv4.

For DS-Lite, the traffic matching and action are applied to inside IPv4 addresses after removing the IPv6 header.

If the matching traffic is for a current full-cone session or user-quota session, and the session uses a different pool or pool group than the one redirected to by the rule list, the rule list is not used.

The **snat pool** option applies only if the client does not have a NAT session. If the client already has a NAT session, the sticky NAT feature keeps the client on the same NAT address, regardless of the LSN rule-list configuration. The option is not applicable to Fixed-NAT (Fixed-NAT44, Fixed-NAT64 or Fixed-NAT for DS-Lite). For these features, the option is ignored and the traffic is dropped. (For drop statistics, refer the "Fixed NAT Dest Rules List Source NAT Drop" counter in the output of the **show cgnv6 fixed-nat statistics** command.

The **one-to-one-snat** option is not applicable to DS-Lite. For these features, the option is ignored and the traffic is processed based only on source IP address. (No rule list is applied.)

Default and Specific Rules

In an LSN rule list, you can configure the following types of rules:

- Rules for specific IP addresses or subnets
- Domain name
- Default rules

If traffic matches an IP-specific rule, that rule is used. Otherwise, the default rules (if configured), are used to match.

If traffic does not have a match in IP-specific rules or the default rule list, the traffic is processed based only on source IP address. (No rule list is applied.)

Example

The following example shows Destination NAT action with domain name for each rule set:

```
ACOS(config)# cgnv6 lsn-rule-list 1
ACOS(config-lsn-rule-list)# ip 1.1.1.1/32
ACOS(config-lsn-rule-list-ip)# tcp port 0 action dnat domain
a10rocks.com
ACOS(config-lsn-rule-list-ip)# udp port 0 action dnat domain
a10rocks.com
ACOS(config-lsn-rule-list-ip)# icmp action dnat domain
a10rocks.com
ACOS(config-lsn-rule-list-ip)# others action dnat domain
a10rocks.com
```

Example The following example shows Destination NAT action with domain name for default rule set:

```
ACOS(config)# cgnv6 lsn-rule-list 1
ACOS(config-lsn-rule-list)# ip 1.1.1.1/32
ACOS(config-lsn-rule-list-ip)# default action dnat domain
a10rocks.com
```

Related Commands:

- cgnv6 template http-alg
- cgnv6 nat icmp always-source-nat-errors

cgnv6 nat icmp always-source-nat-errors

Description Enables NAT for ICMP messages from inside routers.

Syntax

```
[no] cgnv6 nat icmp always-source-nat-errors
```

Default By default, the ACOS device does not translate the source IP addresses of ICMP error messages sent by inside routers into NAT addresses.

Mode Configuration mode

cgnv6 nat icmp respond-to-ping

Description Enables ping replies from NAT pool addresses.

Syntax

```
[no] cgnv6 nat icmp respond-to-ping
```

Default By default, the ACOS device does not reply to ping requests that are sent to NAT addresses (LSN NAT pool addresses). Instead, by default, the ACOS device drops ping requests sent to LSN NAT pool addresses.

Mode Configuration mode

cgnv6 nat icmpv6 respond-to-ping

Description Enables ping replies from NAT pool addresses.

Syntax

```
[no] cgnv6 nat icmpv6 respond-to-ping
```

Default By default, the ACOS device does not reply to ping requests that are sent to NAT addresses (LSN NAT pool addresses). Instead, by default, the ACOS device drops ping requests sent to LSN NAT pool addresses.

Mode Configuration mode

cgnv6 nat inside source static

Description Performs inside configuration for NAT.

Syntax

```
[no] cgnv6 nat inside source static source-addr nat-addr [vrid
 num]
```

Default None.

Mode Configuration mode

Example The following commands configures inside configuration for NAT:

```
ACOS(config)# cgnv6 nat inside source static 1.1.1.1 1.1.1.1
vrid 1
```

cgnv6 nat inside source static partition

Description Performs inside configuration for NAT for inside user partition.

Syntax

```
[no] cgnv6 nat inside source static partition name ipaddr
[vrid  num]
```

Default None.

Mode Configuration mode

Example The following commands configures inside configuration for NAT:

```
ACOS(config)# cgnv6 nat inside source static 1.1.1.1 partition
TEMP 1.1.1.1 vrid 1
```

cgnv6 nat pool

Description Configures a named set of IP addresses for use by Carrier Grade NAT (CGN) or Large Scale NAT (LSN).

Syntax

```
[no] cgnv6 nat pool pool-name
start-ipaddr end-ipaddr
netmask {subnet-mask | /mask-length}
```

```
[max-users-per-ip num]
[port-batch-v2-size {64 | 128 | 256 | 512 | 1024 | 2048 |
4096}]
[shared {all | group | partition}]
[vrid vrid]
```

Syntax

```
[no] cgnv6 nat pool pool-name
start-ipaddr
netmask {subnet-mask | /mask-length}
[max-users-per-ip num]
[port-batch-v2-size {64 | 128 | 256 | 512 | 1024 | 2048 |
4096}]
[shared {all | group | partition}]
[vrid vrid]
```

Syntax

```
[no] cgnv6 nat pool pool-name exclude-ip
start-ipaddr [to end-ipaddr]
```

NOTE: Using the second form of the command shown above, you can configure an address range in a CGN pool by entering a starting address followed by the mask length. This allows use of addresses that use non-zero values in the host portion.

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | **/***mask-length*}	The **netmask** **/***mask-length* option specifies the network mask. All addresses within the resulting subnet are members of the pool, and can be used by CGN for client mappings.
max-users-per-ip *num*	Enables the pool to be used for Large Scale NAT (LSN). The **max-user-per-ip** option specifies the maximum number of internal addresses that can be mapped to a single public address at the same time. You can specify 1-64512. By default, there is no limit.
port-batch-v2-size {**64** | **128**	Configure batched port allocation. The following options are available:

Parameter	Description
| **256** | **512** | **1024** | **2048** | **4096**}	• **per-batch-port-usage-warning-threshold** configures warning log threshold for per batch port usage (default: disabled). • **simultaneous-batch-allocation** allocates the same TCP and UDP batches at once. • **tcp-time-wait-interval** configures the number of minutes before TCP NAT ports can be reused. • **usable-nat-ports** configures usable NAT ports. Under each of these options, the following are the sub-options: • **simultaneous-batch-allocation** allocates same TCP and UDP batches at once. • **tcp-time-wait-interval** configures the minutes before TCP NAT ports can be reused. • **usable-nat-ports** configures usable NAT ports.
shared	Allows L3V partitions running CGN to use this pool. The available options are: • **all** – Shares with all partitions. • **group** – Shares with a partition group. • **partition** – Shares with a single partition.
vrid *vrid*	Adds the resource to a VRRP-A virtual router, identified by its virtual router ID (VRID). The available options are: • **max-users-per-ip**

Parameter	Description
	• **port-batch-v2-size** • **shared**
exclude-ip *start-ipaddr* [**to** *end-ipaddr*]	Excludes the specified IP address or address range from the pool.

Default None.

Mode Configuration mode

cgnv6 nat pool-group

Description Configures a set of IP pools for use by NAT. Pool groups enable you to use non-contiguous IP address ranges, by combining multiple IP address pools.

Syntax

```
[no] cgnv6 nat pool-grouppool-group-name
[vrid vrid]
```

Parameter	Description
pool-group-name	Name of the pool group.
vrid*vrid*	Adds the resource to a VRRP-A virtual router, identified by its virtual router ID (VRID).

This command changes the CLI to the configuration level for the specified pool group, where the following command is available.

(The other commands are common to all CLI configuration levels.)

Command	Description
member *pool-name*	Name of a configured IP address pool.

Default None.

Mode Configuration mode

Usage To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

If a pool group contains pools in different subnets, the ACOS device selects the pool that matches the outbound subnet. For example, of there are two routes to a given destination, in different subnets, and the pool group has a pool for one of those subnets, the ACOS selects the pool that is in the subnet for the outbound route.

The ACOS device selects the pool whose addresses are in the same subnet as the next-hop interface used by the data route table to reach the server.

Example The following commands create a pool group for LSN and add 25 pools to the group:

```
ACOS(config)# cgnv6 nat pool-group group1
ACOS(config-pool-group)# member pool1
ACOS(config-pool-group)# member pool2
ACOS(config-pool-group)# member pool3
...
ACOS(config-pool-group)# member pool25
```

cgnv6 nat range-list

Description Configure an IP source NAT static range list.

Syntax

```
[no] cgnv6 nat range-list list-name
start-ipaddr
netmask {subnet-mask | /mask-length}
start-ipaddr
netmask {subnet-mask | /mask-length}
count number
```

Default None.

Mode Configuration mode

Example The following command configures an IP source NAT static range list:

```
ACOS(config)# cgnv6 nat range-list r1 1.1.1.1 /24 2.2.2.2 /24
count 3
```

Partition is optional. The following command configures an inter-partition scenario:

```
ACOS(config)# cgnv6 nat range-list asasd 11.1.1.1 /24
partition p1 12.2.2.2 /24 count 1
```

cgnv6 nat exclude-port

Description Excludes a specific or a range of ports from the LSN NAT pools in both shared and L3v partitions.

Syntax

```
[no] cgnv6 nat exclude-port tcp | udp
```

Command	Description
tcp	Configures the tcp port from which the specified ports are excluded from the NAT pool.
udp	Configures the udp port from which the specified ports are excluded from the NAT pool.

This command changes the CLI to the configuration level for the specified protocol, where the following command is available.

Command	Description
port	Configures a single port or a starting port range to be excluded from the NAT pool.
to Port Range	Configures an ending port range to be excluded from the NAT pool.

Default tcp

Mode Configuration mode

Example The following commands exclude a specific port or a range of ports from the LSN NAT pool:

```
ACOS(config)# cgnv6 nat exclude-port tcp
```

```
ACOS(config-exclude-tcp-port)# port 1080
ACOS(config-exclude-tcp-port)# port 1060 to 1063
```

cgnv6 one-to-one mapping-timeout

Description Configure a timeout value for the NAT one-to-one mapping.

Syntax

```
[no] cgnv6 one-to-one mapping-timeout timeout-value
```

The *timeout-value* lets you specify how many minutes before the NAT one-to-one mapping expires. The value ranges from 0 to 180 minutes. Configuring 0 minutes means that the mapping times out immediately when there is no active session using that mapping.

Default Timeout of 10 minutes.

Mode Configuration mode

cgnv6 one-to-one pool

Description Configure a named set of IP addresses for use by one-to-one NAT.

Syntax

```
[no] cgnv6 one-to-one pool pool-name
start-ipaddr end-ipaddr
netmask {subnet-mask | /mask-length}
[shared [group group-name | partition partition-name]]
[vrid vrid]
```

Syntax

```
[no] cgnv6 one-to-one pool pool-name
start-ipaddr
netmask {subnet-mask | /mask-length}
[shared [group group-name | partition partition-name]]
[vrid vrid]
```

NOTE: Using the second form of the command shown above, you can configure an address range in a CGN pool by entering a starting address followed by the mask length. This allows use of addresses that use non-zero values in the host portion

Parameter	Description
pool-name	Name of the address pool.
start-	Beginning (lowest) IP address in the range.

Parameter	Description
ipaddr	
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | **/***mask-length*}	The **netmask** */mask-length* option specifies the network mask. All addresses within the resulting subnet are members of the pool, and can be used by CGN for client mappings.
shared	Allows L3V partitions running CGN to use this pool.
vrid *vrid*	Adds the resource to a VRRP-A virtual router, identified by its virtual router ID (VRID).

Default None

Mode Configuration mode

cgnv6 one-to-one pool-group

Description Configure a set of IP pools for use by NAT. Pool groups enable you to use non-contiguous IP address ranges, by combining multiple IP address pools.

Syntax

```
[no] cgnv6 one-to-one pool-grouppool-group-name
[vrid vrid]
```

Parameter	Description
pool-group-name	Name of the pool group.
vrid*vrid*	Adds the resource to a VRRP-A virtual router, identified by its virtual router ID (VRID).

This command changes the CLI to the configuration level for the specified pool group, where the following command is available.

(The other commands are common to all CLI configuration levels.)

Command	Description
member *pool-name*	Name of a configured IP address pool.

Default None.

Mode Configuration mode

Usage To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

If a pool group contains pools in different subnets, the ACOS device selects the pool that matches the outbound subnet. For example, of there are two routes to a given destination, in different subnets, and the pool group has a pool for one of those subnets, the ACOS selects the pool that is in the subnet for the outbound route.

The ACOS device selects the pool whose addresses are in the same subnet as the next-hop interface used by the data route table to reach the server.

Example The following commands create a pool group for LSN and add 25 pools to the group:

```
ACOS(config)# cgnv6 one-to-one pool-group group1
ACOS(config-pool-group)# member pool1
ACOS(config-pool-group)# member pool2
ACOS(config-pool-group)# member pool3
...
ACOS(config-pool-group)# member pool25
```

cgnv6 port-list

Description Configure CGNV6 port list that contains the mapping between original ports and translated ports.

Syntax

```
[no] cgnv6 port-list name [original-port num to translated-port num]
```

Parameter	Description
original-port	Original port to be translated.
translated-port	Port after translation.

Default None.

Mode Configuration mode

Example The following commands create a port list:

```
ACOS(config)# cgnv6 port-list abc
ACOS(config-port-list)# original-port 80 to translated-port
8080
```

cgnv6 resource-usage

Description Configure CGNV6 resource usage.

Syntax

```
[no] cgnv6 resource-usage {fixed-nat-inside-user-count |
fixed-nat-ip-addr-count | lsn-nat-addr-count |radius-table-
size}
```

Parameter	Description
fixed-nat-inside-user-count	Total configurable CGNV6 Fixed NAT inside users.
fixed-nat-ip-addr-count	Total configurable CGNV6 Fixed NAT addresses
lsn-nat-addr-count	Total configurable CGNV6 NAT Pool addresses
radius-table-size	Total configurable CGNV6 RADIUS Table entries
stateless-entries	Helper size for CGN Stateless Technologies.

Default None.

Mode Configuration mode

cgnv6 sctp rate-limit

Description Configure a traffic rate-limit for SCTP sessions.

Syntax

```
[no] cgnv6 sctp rate-limit {source | destination} ip-addr num
```

Parameter	Description
source	Configure a packet rate-limit per second based on an SCTP session source IP.
destination	Configure a packet rate-limit per second based on an SCTP session destination IP.
ip-addr	Specify the IP address of the source or the destination to rate-limit.
num	Configure the packet rate-limit per second. The packets per second ran range from 1 - 2147483647.

Default None.

Mode Configuration mode.

Usage Use these commands to configure the number of SCTP packets allowed per second, whether originating from the source or from the destination address. If this command is not configured, then there is no packet rate-limit for SCTP traffic.

NOTE: This command is available only on CFW platforms. Additionally, it is not supported on Multi-PU platforms.

cgnv6 template http-alg

Description Configure a template for HTTP Application Level Gateway (ALG).

NOTE: The request-insert-msisdn option in HTTP-ALG templates no longer requires a RADIUS service group to be specified.

Syntax

```
[no] cgnv6 template http-algtemplate-name
```

Replace *template-name* with the name of the template, 1-63 characters., of the NAT HTTP-ALG template.

This command changes the CLI to the configuration level for the template, where the following commands are available.

(The other commands are common to all CLI configuration levels.)

Command	Description
[**no**] **request-insert-client-ip** [*options*]	Enables insertion of the client IP address into the headers of client HTTP requests. You can specify the following options: • **header-name** *string* – Header name to insert, instead of the default. • **include-tunnel-ip** – Includes the tunnel IP Address in the inserted header. This option applies only to DS-Lite sessions and 6rd-NAT64 sessions. • **method** {**append** | **replace**} [**header-name** *string* | **include-tunnel-ip header-name** *string*] – Method to use for adding the header: ◦ **append** – Adds a new header field to the end of all the request headers, regardless of how many headers are already in the request. For example, if **append** is configured and header name field displays the default, "X-Forwarded-For," the new "X-Forwarded-For" header will be added to the end of all the headers in the HTTP request. If **append** is configured and header-name is "X-Client-IP," the new "X-Client-IP" will be added to the end of all the headers in the HTTP request. ◦ **replace** – Substitutes the configured header. For example, if **replace** is configured and header-name is default, "X-Forwarded-For," it will be replaced by the new "X-Forwarded-For" header in the HTTP request. If **replace** is configured and header-

Command	Description
	name is “X-Client-IP,” it will be replaced by the new “X-Client-IP” in the HTTP request. If the packet has more than one header field of the same name, all of them will be replaced.
[**no**] **request-insert-msisdn** [*options*]	Inserts the client’s mobile number in client requests. • **header-name***string* – Header name to insert, instead of the default. The following option is available: ◦ **radius-sg***group-name* **secret***string shared-secret* – Specifies the group of RADIUS accounting servers to use for obtaining client mobile numbers. • **radius-sg***group-name* **secret***string shared-secret* – Specifies the group of RADIUS accounting servers to use for obtaining client mobile numbers. The following parameters are available: ◦ *group-name* – Name of the service group that contains the client RADIUS servers. ◦ *string* – Authentication string the ACOS device and the client RADIUS servers use to authenticate RADIUS traffic from one another. ◦ **retry***num* – Maximum number of additional times to send the request, if it times out. You can specify 0-3. The default is 2. ◦ **retry-svr-num***num* – Number of additional servers that can be tried, if the first server does not respond after all retries have timed out. You can specify 0 or 1. The default is 0. ◦ **timeout***seconds* – Maximum number of seconds ACOS waits for the server to reply, before trying again, trying another server (if applicable), or

Command	Description
	giving up. You can specify 1-3 seconds. The default is 2.

Default Not set. When you configure an HTTP-ALG template, the default header for client IP addresses is X-Forwarded-For. The other parameters do not have default settings.

Mode Configuration mode

Example The following commands configure the HTTP-ALG template for insertion of client IP in HTTP requests:

```
ACOS(config)# cgnv6 template http-alg TEMP
ACOS(config-http-alg:TEMP)# request-insert-client-ip header-name TEMP include-tunnel-ip method append
```

Example The following commands configure the HTTP-ALG template for insertion of client mobile number in HTTP requests:

```
ACOS(config)# cgnv6 template http-alg CLIENT-MOBILE-INSERT
ACOS(config-http-alg)# request-insert-msisdn header-name TEMP radius-sg TEMP secret encrypted TEMP retry 0 retry-svr-num 0 timeout 1
```

cgnv6 translation

Description Configure default idle-timeout values for services and protocol traffic over LSN.

Syntax

```
[no] cgnv6 translation
{
icmp-timeout {num | fast} |
service-timeout {tcp | udp} port num {num | fast} |
tcp-timeout num |
udp-timeout num
}
```

Parameter	Description
icmp-timeout {*num* | **fast**}	Configure an idle-timeout or fast aging for ICMP traffic. You can specify a value in the range of 2-

Parameter	Description
	15000 seconds, or **fast**. The **fast** option terminates the session as soon as a response is received.
service-timeout {**tcp** | **udp**} **port** *num* {*num* | **fast**}	Configure an idle-timeout or fast aging for specific services on a port. You can specify a value in the range of 2-15000 seconds, or **fast**. The **fast** option terminates the session as soon as a response is received. By default, this timeout value is not set. For all service ports except UDP 53, the **tcp-timeout** or **udp-timeout** setting is used. For UDP port 53, the Maximum Session Life (MSL) setting is used. **NOTE**: In a CGNv6 only deployment, DNS ALG is enabled by default. As a result, the UDP port 53 DNS session is deleted as soon as the DNS response is received.
tcp-timeout *num*	Configure an idle-timeout for TCP traffic. You can specify a value in the range of 2-15000 seconds.
udp-timeout *num*	Configure an idle-timeout for UDP traffic. You can specify a value in the range of 2-15000 seconds.

Default The default value for **tcp-timeout** and **udp-timeout** is 300 seconds.

Mode Configuration mode

ip-list

Description Configure a list of client addresses. IP lists can be used with features such as Fixed-NAT and client mobile number logging.

Syntax

```
[no] ip-list list-name
```

This command changes the CLI to the configuration level for the specified IP list, where the following command is available.

Command	Description
[**no**] *start-ipv4-addr***to***end-ipv4-addr*	Range of IPv4 addresses. Enter the lowest address number in the range first.
[**no**] *start-ipv6-addr***to***end-ipv6-addr*	Range of IPv6 addresses. Enter the lowest address number in the range first.

Default None

Mode Configuration mode

Example The following commands configure an IP list. The IP list contains the IP addresses of the RADIUS servers.

```
ACOS(config)# ip-list RADIUS_IP_LIST
ACOS(config-ip list)# 40.40.40.1 to 40.40.40.2
ACOS(config-ip list)# exit
```

Within an IP-list entry, you can specify prefixes in any of the following ways:

- Range – Specify the starting prefix and ending prefix in the range. Example: `4001::/32 to 4025::/32`
- Count – Specify the starting prefix, and the total number of prefixes for the entry. The count can be 1-2147483647. Example: `6001::/16 count 1000`
- Single prefix – Example: `2001:DB8::/32`

The following commands configure an IP list that contains some IPv6 prefix entries:

```
ACOS(config)# ip-list test
ACOS(config-ip list)# 6001::/16 count 1000
ACOS(config-ip list)# 4001::/32 to 4025::/32
ACOS(config-ip list)# 3001::1 to 3001::100
```

The first two commands configure prefix ranges. The last command configures a unicast address range.

netflow monitor

Description Enable the ACOS device to act as a NetFlow exporter, for monitoring traffic and exporting the data to one or more NetFlow collectors for analysis.

Syntax

```
[no] netflow monitor monitor-name
```

Replace *monitor-name* with the name of the NetFlow monitor.

This command changes the CLI to the configuration level for the specified NetFlow monitor, where the following commands are available.

Command	Parameter
[no] **destination** {**service-group** *sg-name* | *ip-addr*}	Configure the destination where NetFlow records will be sent by entering a service group (if using multiple NetFlow collectors), or an IP address for a specific host.
disable	Disable this NetFlow monitor.
disable-log-by-destination	Disable logging by destination protocol and port. The following options are available: • **icmp** – Disable logging for icmp traffic. • **others** – Disable logging for other L4 protocols. • **tcp** – Disable logging by destination TCP port. • **udp** – Disable logging by destination UDP port.
[no] **flow-timeout** *minutes*	Timeout value interval at which flow records will be periodically exported for long-lived sessions. Flow records for short-lived sessions (if any) are sent upon termination of the session. After the specified amount of time has elapsed, the ACOS device will send any flow records to the NetFlow collector, even if the flow is still active. The flow timeout can be set to 0-1440 minutes. The

Command	Parameter
	flow timeout default value is 10 minutes. Setting the timeout value to 0 disables the flow timeout feature. Regardless of how long-lived a flow might be, the ACOS device waits until the flow has ended and the session is deleted before it sends any flow records for it.
[**no**] **protocol** {**v9** | **v10**}	Configure which version of the NetFlow protocol to use, version 9 or version 10. The default is NetFlow version 9.
[**no**] **record** *netflow-template-type* [**both** | **creation** | **deletion**]	Configure the NetFlow record types to be exported. (For more information, see "NetFlow v9 and v10 (IPFIX)" topic in the System Configuration and Administration Guide.) The netflow-template-type refers to the NetFlow template that defines the NetFlow records to export, and it includes the following template types: • dslite – DS-Lite Flow Record Template • nat44 – NAT44 Flow Record Template • nat64 – NAT64 Flow Record Template • netflow-v5 – NetFlow V5 Flow Record Template • netflow-v5-ext – Extended NetFlow V5 Flow Record Template, supports ipv6 • port-batch-dslite – DS-Lite Port Batching Event Template • port-batch-nat44 – NAT44 Port Batching Event Template • port-batch-nat64 – NAT64 Port Batching Event Template • port-batch-v2-dslite – DS-Lite NAT Port Batching

Command	Parameter
	v2 Event Template • port-batch-v2-nat44 – NAT44 NAT Port Batching v2 Event Template • port-batch-v2-nat64 – NAT64 NAT Port Batching v2 Event Template • port-mapping-dslite – DS-Lite Port Mapping Event Template • port-mapping-nat44 – NAT44 Port Mapping Event Template • port-mapping-nat64 – NAT64 Port Mapping Event Template • sesn-event-dslite – DS-Lite Session Event Template • sesn-event-nat44 – NAT44 Session Event Template • sesn-event-nat64 – NAT64 Flow Record Template The options for specifying **both**, **creation**, and **deletion** allow you to determine which types of events will be exported: • **both** – Export both creation and deletion events (default) • **creation** – Export only creation events • **deletion** – Export only deletion events The **both**, **creation**, and **deletion** options are only available for session event and port mapping event templates. They are not available for flow record templates.
[**no**] **resend-**	Configure when to resend the NetFlow template.

Command	Parameter
template {**records** *num* | **timeout** *seconds*}	The trigger can be either the number of records, or the amount of time that has passed. • **records** – Specify a range from 0-1000000, with a default of 1000 records. Note that specifying 0 means never resend the template. • **timeout** – Specify a range from 0-86400, with a default of 1800 records. Note that specifying 0 means never resend the template.
[no] **source-address** {**ip** *string* | **ipv6** *string*}	Specify the IPv4 or IPv6 source address of the Netflow packet. • **ip** – Specify the source address in the ipv4-address format of A.B.C.D. • **ipv6** – Specify the source address in the ipv6-address format of A:B:C:D:E:F:G:H.
[**no**] **source-ip-use-mgmt**	Use the management interface's IP address as the source IP for exported NetFlow packets. Note that this command does not change the ACOS port from which NetFlow traffic is exported.

Default Described above, where applicable.

Mode Configuration mode

Usage A NetFlow monitor consists of the following protocol parameters, which can be used to configure the ACOS device to export data in the format of NetFlow v9 or NetFlow v10 (IPFIX). The current release supports NetFlow version 9 (RFC 3954), and NetFlow version 10 (IPFIX) (RFC 5101).

You can configure up to 64 NetFlow monitors.

NOTE: When configuring the **netflow monitor** command, the system may experience high CPU utilization if the sampling rate is too low or if multiple interfaces are being monitored with high traffic. It is recommended to adjust the sampling rate and monitor to optimize performance.

Limitation

NetFlow Ethernet filters are not supported when used with ADC.

Predefined NetFlow Templates

The ACOS device includes some pre-defined NetFlow templates. For more information, see "NetFlow v9 and v10 (IPFIX)" topic in the IPv4-to-IPv6 Transition Solutions Guide.

session-filter

Description Configure a session filter.

Syntax

```
session-filterfilter-name set
{
dest-addrportnum |
dest-portportnum |
ipv6 |
sip |
source-addrportnum |
source-portportnum
}
```

Parameter	Description
dest-addr*portnum*	Matches on destination address.
dest-port*portnum*	Matches on destination port.
ipv6	Matches specifically on IPv6 addresses.
sip	Matches on SIP sessions.
source-addr*portnum*	Matches on source address.
source-port*portnum*	Matches on source port.

Default No session filters are configured by default.

Mode Configuration mode

Usage Session filters allows you to save session display options for use with the **clear session** and **show session** commands. Configuring a session filter allows you to specify a given set of options one time rather than re-entering the options each time you use the **clear session** or **show session** command.

Example The following example sets session filter criteria of a forward destination IP and forward destination port:

```
ACOS(config)# session-filter TEMP set dest-addr 1.1.1.1 dest-port 1
```

DNS64

cgnv6 nat pool

Description Configure an IPv4 pool, for DNS64 to use while acting as a proxy for a local IPv4 DNS server. For syntax information, see cgnv6 nat pool.

cgnv6 nat pool-group

Description Configure a set of IP pools for use by NAT. Pool groups enable you to use non-contiguous IP address ranges, by combining multiple IP address pools. For syntax information, see cgnv6 nat pool-group.

cgnv6 nat64 prefix

Description Configure the NAT64 prefix.

Syntax

```
[no] cgnv6 nat64 prefix ipv6-addr/nn
[class-list list-name] | follow-nat-pool-vrid |
[vrid vrid]
```

Parameter	Description
ipv6-addr/nn	Specifies the prefix.
class-list *list-name*	Specifies a class list of inside source parameters for the prefix.

Parameter	Description
follow-nat-pool-vrid	Allows NAT64 to use a virtual router ID (VRID) configured under the NAT pool to enable NAT64 VRRP active-active mode.
vrid *vrid*	Adds the resource to a VRRP-A virtual router, identified by its virtual router ID (VRID).

Default The default is 64:ff9b::/96. No VRID is assigned by default.

Mode Configuration mode

cgnv6 server

Description Configure the local DNS server to be proxied.

Syntax

```
[no] cgnv6 server server-name {ipaddr | ipv6-addr}
```

This command creates the server and changes the CLI to the configuration level for the server, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[**no**] **health-check** {*monitor-name*}	Enables health monitoring of the server. The **monitor-name** specifies the name of a configured health monitor. If you omit this command or you enter it without the **monitor-name** option, the default Layer 3 (ICMP) health monitor is used.
[**no**] **health-check-disable**	Disables health monitoring of the server.
[**no**] **port**	Specifies the TCP or UDP port on which the server listens for traffic.

Command	Description
port-num {**tcp** | **udp**}	**enable | disable** Enables or disables the port. [**no**] **health-check** [*monitor-name*] Enables health monitoring of the port. The monitor-name option specifies the name of a configured health monitor. If you omit the **health-check** command or you enter it without the monitor-name option, the default UDP health monitor is used. [**no**] **health-check-disable** Disables health monitoring of the port.

Default None

Mode Configuration mode

Usage The normal form of the **cgnv6 server** command creates a new real server or edits an existing real server. The CLI changes to the configuration level for the server. The "**no**" form of this command removes an existing real server. The IP address of the server can be in either IPv4 or IPv6 format. ACOS devices support both address formats.

Default Health Monitoring

The following health monitors are enabled by default.

- ICMP – Server health check. Every 5 seconds, the ACOS device sends an ICMP echo request (ping) addressed to the server's IP address. The server passes the health check if it sends an echo reply to the ACOS device. If the server does not reply after the fourth attempt (the first attempt followed by 3 retries), the ACOS device sets the server state to DOWN.
- UDP – Protocol port health check. Every 5 seconds, the ACOS device sends a packet with a valid UDP header and a garbage payload to the UDP port. The port passes the health check if the

server either does not reply, or replies with any type of packet except an ICMP Error message.

cgnv6 service-group

Description Configure a service group, which is a pool of one or more servers.

Syntax

```
[no] cgnv6 service-group group-name {tcp | udp}
```

Replace *group-name* with the name of the group, 1-31 characters.

This command changes the CLI to the configuration level for the specified service-group, where the following command is available:

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] health-check *[monitor-name]*	Enables health monitoring of the service group. The **monitor-name** specifies the name of a configured health monitor.
[no] member *{member-name} {portnum}*	Adds the external log server and port to the service group.
[no] shared {group | partition}	Configures the service group to share with either a partition group or a single partition.

Default There are no service groups configured by default.

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing service group. The CLI changes to the configuration level for the service group.

cgnv6 template dns

Description Configure a DNS template to enable DNS64 and set DNS64 options.

Syntax

```
[no] cgnv6 template dns template-name
```

This command creates the template and changes the CLI to the configuration level for the template, where the following DNS64-related commands is available:

The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] **class-list** *class-list* **lid** *num* {**conn-rate-limit** | **over-limit-action**}	Enables health monitoring of the service group. The **monitor-name** specifies the name of a configured health monitor. • **conn-rate-limit** configures the connection rate limit. • dns configures DNS cache options. The following options are available: • **cache-disable** disables DNS cache. • **cache-enable** enables DNS cache. • **ttl** configures TTL for cache entry. • **weight** configures weight for cache entry. • **over-limit-action** configures the action when the connection rate limit is exceeded. The following actions are available: ◦ **dns-cache-disable** disables DNS cache when it exceeds limit. ◦ **dns-cache-enable** enables DNS cache when it exceeds limit. ◦ **forward** forwards the traffic even it exceeds limit. ◦ **lockout** Any new connection for certain time will not be accepted. ◦ **log** logs a message.

Command	Description
[no] **default-policy** [**nocache** | **cache**]	Specify the default action to take when a query does not match any class-list entries.
[no] **disable-dns-template**	Disables the DNS template.
[no] dns-log-enable period *period*	Specify how often log messages are generated for DNS caching. (1-10000 minutes)
[no] **dns64**	Enables or disables DNS64. This option is disabled by default. The following options are available: • **answer-only-disable** If you configure this command, the IPv4 addresses in all sections of DNS replies are synthesized to IPv6. Otherwise, the ACOS device synthesizes IPv6 address for only resource records in the ANSWER section of DNS replies. When the **dns64** option is enabled, this sub-option is enabled. • **auth-data** When the ACOS device receives an A-query-response from the DNS server, this option sets the authenticated-data bit in synthesized AAAA responses. The auth-bit will be set only if DNS64 synthesis is performed in the reply. Otherwise, the bit will not be changed. When the **dns64** option is enabled, this sub-option is disabled. • **cache** Uses a cached A-query response to provide AAAA query responses for the same hostname, without consulting the DNS server. When the **dns64** option is enabled, this sub-option is disabled.

Command	Description
	For example, assume that an A query has been cached for hostname example.com. If the client sends a AAAA query for example.com, the ACOS device does not consult the DNS server. Instead, the ACOS device uses the cached type A answer to synthesize a AAAA response, and sends the synthesized response to the client. • **change-query** When the ACOS device receives a AAAA request from a client, this option forwards only an A request on behalf of the client. This option saves time if the DNS database only contains A records, because the ACOS device does not need to wait for an error or empty response, or for the response to time out. When the **dns64** option is enabled, this sub-option is disabled. • **compress-disable** Saves network costs by compressing DNS packets. When the **dns64** option is enabled, this sub-option is enabled. • **deep-check-rr-disable [drop-cname-disable]** Evaluates the resource records in the ANSWER sections of DNS replies individually. Sometimes the DNS server may send only CNAMEs in the ANSWER section in response to a AAAA query. This option drops such responses, considering them to be empty, and initiates an A query towards the hostname. By default, this option is enabled. This option is valid only when the deep-check-RR option is enabled. When the **dns64** option is enabled, this sub-option is enabled. • **enable** Enables DNS64.
[**no**] **dns64**	• **ignore-rcode3-disable** Ignores any DNS response with rcode 3 in response to a AAAA query. The ACOS device treats the response as empty, and sends an A

Command	Description
	query to the same hostname. This option is useful for circumventing DNS servers that are configured incorrectly to return rcode=3 when they do not have any AAAA records for the hostname, even though the hostname exists. When the **dns64** option is enabled, this sub-option is enabled. • **max-qr-length** *num* Forwards the response from the DNS server to the client without any modification to the response, if the question-record length is greater than the specified length. The length can be 1-1023 bytes. When the **dns64** option is enabled, this value is set to 128 by default. • **parallel-query** Sends both an IPv6 AAAA request and an IPv4 A request in parallel (at the same time) on behalf of the client. When this option is enabled, the ACOS device performs DNS64 synthesis if necessary, and forwards the first valid response received to the client. (Empty responses and errors are invalid.) If both responses are invalid, the ACOS device forwards the last invalid response to the client. When the **dns64** option is enabled, this sub-option is disabled. **NOTE:** It is recommended to disable passive queries (**passive-query disable**) and the single-response option enabled (no single response-disable) when using the **parallel-query** option. • **passive-query-disable** Initiates an A query upon receiving an empty response or error for a AAAA query. When the **dns64** option is enabled, this sub-option is enabled.

Command	Description
	• **retry** *retry-num* Specifies the maximum number of times the ACOS device will retry an A query if a response is not received from the DNS server. You can specify 0-15. If you specify 0, retries are disabled. When the **dns64** option is enabled, this value is set to 3 by default. • **single-response-disable** When the ACOS device is operating in parallel-query mode, the ACOS device will send two queries to the DNS server at the same time. Both queries could come back with valid responses. When the **dns64** option is enabled, this sub-option is enabled. When the single-response option is enabled, the first valid response is forwarded to the client. If two invalid responses are received, the last one is forwarded to the client. If you disable this option, the ACOS device will forward both responses to the server, if both responses are valid. • **timeout** *seconds* Specifies the maximum number of seconds the ACOS device waits for a AAAA response before sending an A query. You can specify 0-15 seconds. When the **dns64** option is enabled, this value is set to 1 by default.
[**no**] **dns64**	• **trans-ptr** [**trans-ptr-query**] Enables you to run PTR queries for synthesized IPv6 addresses with the client. The PTR queries are intercepted by DNS64 and converted into PTR queries for their corresponding IPv4 addresses before sending out. When the response is received by the ACOS device, the response is synthesized and sent back to the client as if it were a response for the synthesized

Command	Description
	IPv6 address. When the **dns64** option is enabled, this sub-option is disabled. • **ttl** *seconds* Specifies the maximum TTL to use in synthesized AAAA replies, in place of the TTL value in the original IPv4 DNS reply. ◦ If the TTL value in the template is lower than the TTL value in the IPv4 reply, the template's TTL value is used in the synthesized IPv6 reply. ◦ If the TTL value in the template is equal to or higher than the TTL value in the IPv4 reply, the TTL value in the IPv4 reply is used in the synthesized IPv6 reply. You can specify 1-1000000000 seconds. When the **dns64** option is enabled, this sub-option is not set by default.
[**no**] **malformed-query** {**drop** | **forward** *service-group-name*}	Specifies the action the ACOS device will take on malformed queries. • **drop** - the malformed query will be dropped • **forward** - the malformed query will be forwarded to a service group.
[**no**] **max-cache-size** *num*	Specify the maximum number of entries that can be cached per VIP. **NOTE:** The maximum configurable amount depends on the amount of RAM installed on the ACOS device.

Default None.

Mode Configuration mode

cgnv6 dns64-virtualserver

Description Configure the virtual server for the DNS proxy, to which clients will send DNS queries.

Syntax `[no] cgnv6 dns64-virtualserver name {ipaddr | ipv6-addr}`

This command creates the server and changes the CLI to the configuration level for the virtual server, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
`[no] port port-number dns-udp`	Specifies the UDP port number and the port type, **dns-udp**. This command changes the CLI to the configuration level for the port, where the following commands are available: • **service-group** *group-name* Binds the virtual port to the service group. • **source-nat** {**auto** | **pool**} Binds the virtual port on an IP NAT pool or pool group. Use the **auto** option to configure auto NAT for the vport. Use the **pool** option to specify NAT pool or pool group. • **template dns** *template-name* • Binds the virtual port to the DNS template containing the DNS64 settings.

Command	Description
	• **template policy** *template-name* Binds the virtual port to a policy template, if applicable. • **enable** enables the virtual port • **disable** disables the virtual port.
[**no**] **template policy** *template-name*	Binds a policy template to the virtual server, if applicable.
[**no**] **vrid***vrid*	Adds the virtual server to a VRRP-A group.
enable	Enables the virtual server.
disable	Disables the virtual server.

Default None

Mode DNS template configuration.

Example This example shows how to use an IP NAT pool with DNS64:

```
ACOS(config)# ip nat pool rr1 10.10.10.1 10.10.10.10 netmask
/24
ACOS(config)# cgnv6 dns64-virtualserver dns64 20.1.1.20
ACOS(config-cgnv6 dnsvserver)# port 53 dns-udp
ACOS(config-cgnv6 dnsvserver-vport)# source-nat pool rr1
```

Related Commands:

- cgnv6 template dns
- cgnv6 template policy

NAT64

cgnv6 ecmp 4-tuple-hash

NOTE: For information on this command, see cgnv6 ecmp 4-tuple-hash"

class-list (for NAT64)

Description Configure a class list that specifies IPv6 addresses or prefixes on which to perform an override action. For matching entries, the override action is applied instead of the configured NAT64 action.

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a standalone file on the ACOS device.

NOTE: A class list can be exported only if you use the **file** option.

This command changes the CLI to the configuration level for the specified class list, where the following command is available.

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[**no**] *ipv6-addr*/*prefix* {**glid** | **lid** | **lsn-lid**} *num*	Adds an entry to the class list. • *ipv6-addr*/*prefix* – Specifies an IPv6 address or prefix on which to perform an override action • {**glid** | **lid**} *num* – Specifies a Global Limit ID (GLID) or a Limit ID (LID) configured in a policy template. These

Command	Description
	options apply only to NAT64 override. • **lsn-lid** *num* – Specifies the LID that refers to the NAT pool (or group of pools) containing the IPv4 address(es) to use for NATting traffic from IPv6 clients to IPv4 servers.

Default None

Mode Configuration mode

Usage Use glid (for NAT64 override) if you plan to use a GLID.
Use cgnv6 template policy if you plan to use a policy template instead.

glid (for NAT64 override)

Description Configure a GLID to specify a NAT64 override action.

NOTE: This command applies only for configuring NAT64 override actions. Use cgnv6 lsn-lid to configure the LID for regular NAT64.

Syntax

```
[no] glid num
```

Replace *num* with the GLID number, 1-1023.

This command changes the CLI to the configuration level for the specified GLID, where the following command is available.

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] dns64 {disable | exclusive-answer |	Specifies the override action: • **disable** – Does not perform DNS64 processing on the client's DNS

Command	Description
prefix *ipv6-addr/nn}*	request. The client's request is forwarded to the DNS server, and the reply is sent to client without modification. • **exclusive-answer** – Drops AAAA replies that contain specific IPv6 addresses or prefixes. In this case, the ACOS device sends an A query on behalf of the client, then uses DNS64 to add synthesized IPv6 addresses in the reply before sending the reply to the client. • **prefix** *ipv6-addr/nn* – Uses a different NAT64 prefix to synthesize IPv6 addresses in the reply to the client. You can use this option to load balance NAT64 service across multiple ACOS devices.

Default None

Mode Configuration mode

cgnv6 nat pool (for NAT64)

Description Configure a NAT pool containing the IPv4 address(es) to use for NATting traffic from IPv6 clients to IPv4 servers.

Related Commands:

- cgnv6 nat pool

cgnv6 nat pool-group (for NAT64)

Description Configure a set of IP pools for use by NAT. Pool groups enable you to use non-contiguous IP address ranges, by combining multiple IP address pools.

Related Commands:

- cgnv6 nat pool-group

cgnv6 lsn-lid

Description Configure a Limit ID (LID) for NAT64. This LID will refer to the NAT pool (or group of pools) containing the IPv4 address(es) to use for NATting traffic from IPv6 clients to IPv4 servers.

NOTE: This command is not applicable to GLIDs or LIDs used for configuring NAT64 override actions. To configure a GLID or LID for NAT64 override, see glid (for NAT64 override) or cgnv6 template policy.

Syntax

```
[no] cgnv6 lsn-lid num
```

Replace *num* with the LID number, 1-31.

This command changes the CLI to the configuration level for the specified LID, where the following command is available.

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] **source-nat-pool** *pool-name*	Binds an IPv4 NAT pool to the LID.
[no] **user-quota-prefix-length** *mask-length*	Assign a user quota to all users of a specific IPv6 prefix.

Default None

Mode Configuration mode

cgnv6 nat64 alg

Description Enable or disable Application Level Gateway (ALG) support.

Syntax

```
[no] cgnv6 nat64 alg {esp | ftp [options]| h323 | mgcp| pptp | rtsp | sip | tftp}
{disable | enable}
```

Parameter	Description
esp {**enable** |**disable**}	Enables or disables NAT64 ALG support for Encapsulating Security Payload (ESP).
ftp [*options*]	Enables or disables NAT64 ALG support for File Transfer Protocol (FTP). The options enable or disable command translation for compatibility with old FTP servers. NAT64 FTP ALG supports the following command translations: • **trans-eprt-to-port** – EPRT (RFC 2428) to PORT • **trans-epsv-to-pasv** – EPSV (RFC 2428) to PASV • **trans-lprt-to-port** – LPRT (RFC 1639) to PORT • **trans-lpsv-to-pasv** – LPSV (RFC 1639) to PASV • **xlat-no-trans-pasv** – Skip PASV response. The Payload of the IP address information will not be translated from IPv4 to IPv6
h323 {**enable** | **disable**}	Enables or disables NAT64 ALG support for H323 standard.
mgcp {**enable** | **disable**}	Enables or disables NAT64 ALG support for Media Gateway Control Protocol (MGCP).
pptp {**enable** | **disable**}	Enables or disables NAT64 ALG support for Point-to-Point Tunneling Protocol (PPTP).
rtsp {**enable** | **disable**}	Enables or disables NAT64 ALG support for Real Time Streaming Protocol (RTSP).
sip {**enable** | **disable**}	Enables or disables NAT64 ALG support for Session Initiation Protocol (SIP).

Parameter	Description
tftp {**enable** | **disable**}	Enables or disables NAT64 ALG support for Trivial File Transfer Protocol (TFTP).

Default ALG support for FTP is enabled by default, and all the command translation options are enabled by default except for "**xlat-no-trans-pasv**". ALG support for ESP, H323, MGCP, PPTP, RTSP, SIP, and TFTP is disabled by default.

Mode Configuration mode

cgnv6 nat64 force-non-zero-ipv4-id

Description Enable the Identification field in an IPv4 header to have a non-zero number for non-fragmented IPv6 packets between 88 and 1280 bytes in size.

Syntax

```
cgnv6 nat64 force-non-zero-ipv4-id [all]
```

The **all** option enables the Identification field to have a non-zero number for all packet sizes.

Default Disabled. If the IPv6 packet is not fragmented, the Identification field in the IPv4 header will be 0 by default.

Mode Configuration mode

Usage In some cases, servers will drop packets with a "0" in the Identification field of an IPv4 header when the IPv6 packet is not fragmented. This command forces the IPv4 header to have a non-zero number in that Identification field whenever the IPv6 packet is not fragmented. By default, when enabled, non-zero identification numbers are only applied to packets between 88 and 1280 bytes. Using the optional **all** command at the end configures a non-zero value in the Identification field of the IPv4 packet for all non-fragmented IPv6 packets, regardless of packet size.

cgnv6 nat64 fragmentation df-bit-transparency

Description Enable or disable insertion of headers that have the more-fragments bit set to zero, and that have the fragmentation-offset set to zero.

Syntax

```
[no] cgnv6 nat64 fragmentation df-bit-transparency  enable
```

Default Insertion of headers that have the more-fragments bit set to zero and the fragmentation-offset set to zero is disabled by default.

Mode Configuration mode

Usage This option applies to the IPv4-to-IPv6 traffic direction. When this option is enabled, headers are inserted when the IPv4 Don't Fragment bit is not set.

cgnv6 nat64 fragmentation inbound

Description Configure fragmentation support for inbound packets.

Syntax

```
[no] cgnv6 nat64 fragmentation inbound
{df-set | drop | ipv6}
```

Parameter	Description
df-set	Configures the behavior for inbound fragmented packets when Don't Fragment (DF) bit is set. The following options are available: • **drop** drops silently • **ipv6** uses IPv6 fragmentation. • **send-icmp** sends ICMP Type 3 Code 4. This is the default option.
drop	Drops inbound fragmented packets.
ipv6	Uses IPv6 fragmentation support for inbound oversized packets.

Default The following options are enabled by default:

- ipv6
- df-set send-icmp

Mode Configuration mode

NOTE: If df-set is not configured, then the default is to use ipv6-fragmentation. If df-set is configured, the default is to send back an icmp error.

cgnv6 nat64 fragmentation inbound df-set

Description Configure the behavior for inbound fragmented packets when Don't Fragment (DF) bit is set.

Syntax

```
[no] cgnv6 nat64 fragmentation inbound df-set
{drop | ipv6| send-icmp [count num]}
```

Parameter	Description
send-icmp [**count** *num*]	Enables sending of ICMP unreachable messages for inbound fragmented packets, and disallows overriding the Don't Fragment bit. You can configure the number of ICMP messages sent when DF is set. The default is 1.
drop	Drops inbound fragmented packets. The **df-set** option disallows override of the Don't Fragment bit.
ipv6	Enables fragmentation support for inbound IPv6 packets. The **df-set** option disallows override of the Don't Fragment bit.

Default **df-set send-icmp**

Mode Configuration mode

cgnv6 nat64 fragmentation outbound

Description Configure fragmentation support for outbound packets.

Syntax

```
[no] cgnv6 nat64 fragmentation outbound
{
drop |
ipv4 |
```

```
send-icmpv6
}
```

Parameter	Description
drop	Drops outbound fragmented packets.
ipv4	Allows fragmentation of outbound IPv4 packets.
send-icmpv6	Enables sending of ICMPv6 unreachable messages for outbound IPv6 fragmented packets, and disallows overriding the Don't Fragment bit.

Default **ipv4**

Mode Configuration mode

cgnv6 nat64 icmp

Description Send ICMP Destination Unreachable messages when there are no protocol ports available for NAT mappings, or when a a user quota is exceeded.

Syntax

```
[no] cgnv6 nat64 icmp
{send-on-port-unavailable | send-on-user-quota-exceeded}
{host-unreachable | admin-filtered | disable}
```

Parameter	Description
send-on-port-unavailable	Sends ICMP Destination Unreachable message when there are no protocol ports available for NAT mappings.
send-on-user-quota-exceeded	Sends ICMP Destination Unreachable message when a a user quota is exceeded.
host-unreachable	Sends code type 3, code 1 for IPv4, and type 1 code 3 for IPv6.
admin-filtered	Sends code type 3, code 13, administratively filtered.
disable	Disable ICMP Unreachable messages for the specified event.

Default The default for **send-on-port-unavailable** is **disable**. The default for **Send-on-user-quota-exceeded** is **admin-filtered**.

Mode Configuration mode

cgnv6 nat64 inside

Description Bind a class list to the NAT64 feature.

Syntax

```
[no] cgnv6 nat64 inside source class-list list-name
```

Default None

Mode Configuration mode

Related Commands:

- class-list (for NAT64)

cgnv6 nat64 prefix

Description See cgnv6 nat64 prefix.

cgnv6 nat64 tcp mss-clamp

Description Configure TCP maximum segment size (MSS) clamping. MSS clamping checks the TCP MSS value in IPv4 packets clients and, if necessary, changes it before sending the NATted request to the server.

Syntax

```
[no] cgnv6 nat64 tcp mss-clamp {fixed n | none | subtract s
[min n]}
```

Parameter	Description
fixed *n*	Changes the MSS to the length you specify.
none	Does not change the MSS value.
subtract *s* [**min** *n*]	Reduces the MSS if it is longer than the specified number of bytes. This option sets the MSS based on the following calculations: • If MSS minus S is greater than N, subtract S from the MSS.

Parameter	Description

	• If MSS minus S is less than or equal to N, set the MSS to N.
	
	The subtract method of MSS clamping is used by default, with the following values:
	
	`S = 20 bytes`
	
	`N = 476 bytes`
	
	Using these values, the default MSS clamping calculations are as follows:
	
	• If MSS minus 20 is greater than 476, subtract 20 from the MSS.
	
	• If MSS minus 20 is less than or equal to 476, set the MSS to 476.

Default The **subtract** option is used by default.

Mode Configuration mode

cgnv6 nat64 tcp reset-on-error

Description Send TCP resets to clients in response to invalid TCP packets from the inside network.

Syntax `[no] cgnv6 nat64 tcp reset-on-error outbound disable`

Default Enabled

Mode Configuration mode

cgnv6 nat64 user-quota-prefix-length

Description Assign a user quota to all users of a specific NAT64 prefix.

Syntax `[no] cgnv6 nat64 user-quota-prefix-length mask-length`

Parameter	Description
mask-	Prefix length, 1-

Parameter	Description
length	128.

Default 128

Mode Configuration mode

Usage You can apply a user quota prefix length on a global level or per LSN LID basis. The user quota prefix length set for an LSN LID overrides the global configuration value.

If the user quota prefix length is broader than the subnet to which the LSN LID is bound, the user quota may not be enforced

For the command show cgnv6 nat64 user-quota-sessions, if a user quota prefix length is configured, only the prefix quota is displayed. If the prefix quota is not set, only the user quota session is displayed.

cgnv6 template policy

Description Configure a policy template, to override the configured NAT64 behavior for specific IPv6 addresses or prefixes.

Syntax

```
[no] cgnv6 template policy template-name
```

This command changes the CLI to the configuration level for the specified class list, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] **class-list** *list-name*	Specifies the class list. The following sub-commands are available: • **client-ip** – Set the client IP address. By default, the source IP address is used. ◦ **client-ip l3-dest** - Extract the client's IP address from the

Command	Description
	Layer 7 header, using the destination IP as the client's IP address. ◦ **client-ip l7-header** [*L7-header-name*] – Extract the client's IP address from the layer 7 header, using the name of the Layer 7 header. • **lid** num- Configure a LID within the class list. This command changes the CLI to the configuration level for the LID, where the following sub-command is available: ◦ **conn-limit** configures the connection limit. ◦ **conn-rate-limit** specifies the connection rate limit. ◦ **dns64** {**disable** | **prefix** *ipv6-addr*/*nn* | **exclusive-answer**} applies DNS64. This command specifies the override action for IPv6 addresses that match the class list. The following options are available: **disable** – Does not perform DNS64 processing on the client's DNS request. The client's request is forwarded to the DNS server, and the reply is sent to client without modification. **prefix** *ipv6-addr*/*nn* – Uses a different NAT64 prefix to synthesize IPv6 addresses in the reply to the client. You can use this option to load balance NAT64 service across multiple ACOS devices. **exclusive-answer** – Drops AAAA replies that contain specific IPv6 addresses or prefixes. In this case, the ACOS device sends an

Command	Description
	A query on behalf of the client, then uses DNS64 to add synthesized IPv6 addresses in the reply before sending the reply to the client. • **over-limit-action** sets action when exceeds limit. • **request-limit** sets the request limit. • **request-rate-limit** sets the request rate limit.

Default None

Mode Configuration mode

ip nat inside

Description Enable IPv4 inside NAT on the interface connected to the IPv4 Internet.

Syntax `[no] ip nat inside source {class-list | list | static}`

Default Disabled

Mode Interface configuration level

ip nat-global reset-idle-tcp-conn

Description Enable client and server TCP Resets for NATted TCP sessions that become idle.

Syntax `[no] ip nat-global reset-idle-tcp-conn`

Default Disabled

Mode Configuration mode

ip frag timeout

Description Configures IP fragmentation parameters.

Syntax `{ip | ipv6} frag timeout millisecond`

Default 60000

Mode Configuration mode

Usage This command allows to change the fragment timeout between the receipt of each fragment of a fragmented packet.

ip frag max-reassembly-sessions

Description Configures the maximum number of pending reassembly sessions allowed.

Syntax `ip frag max-reassembly-sessions num`

Default 100000

Mode Configuration mode

Dual-Stack Lite Commands

This section describes the Dual-Stack Lite (DS-Lite) configuration commands. DS-Lite enables the ACOS device to act as an end-point for IPv4 traffic tunneled through an IPv6 link.

class-list (for DS-Lite)

Description Configure an IP class list for use with Dual-Stack Lite (DS-Lite).

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a file.

This command changes the CLI to the configuration level for the specified class list, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to DS-Lite.

Command	Description
[**no**] *ipv6-addr* **/***prefix-length* **lsn-lid** *num*	Adds an entry to the class list. • *ipv6-addr*/*prefix-length* – Specifies the range of client IPv6 addresses on which to match. These are the IPv6 addresses of the customer DS-Lite routers. • **lsn-lid** *num* – Specifies the LID number.

Default None

Mode Configuration mode

Usage Configure the DS-Lite LIDs before configuring the class-list entries. Use cgnv6 nat icmp always-source-nat-errors to configure an LID for DS-Lite.

As an alternative to configuring class entries on the ACOS device, you can configure the class list using a text editor on another device, then import the class list onto the ACOS device.

For more information, see “Dual-Stack Lite” topic in the IPv4-to-IPv6 Transition Solutions Guide.

cgnv6 ds-lite alg

Description Configure Application Level Gateway (ALG) support for DS-Lite.

Syntax

```
[no] cgnv6 ds-lite alg
{ftp | h323 | mgcp | pptp | rtsp | sip | tftp}
{enable | disable}
```

Specify the protocol for which to disable or enable ALG support:

- **ftp** – File Transfer Protocol
- **h323** – H.323 standard is a legacy voice-over-IP (VoIP) protocol.
- **mgcp** – Media Gateway Control Protocol (MGCP)
- **pptp** – Point-to-Point Tunnelling Protocol
- **rtsp** – Real Time Streaming Protocol
- **sip** – Session Initiation Protocol
- **tftp** – Trivial File Transfer Protocol

Default ALG support for FTP is enabled by default. ALG support for the other protocols is disabled by default.

Mode Configuration mode

cgnv6 ds-lite fragmentation inbound

Description Configure fragmentation support for inbound packets.

Syntax

```
[no] cgnv6 ds-lite fragmentation inbound
{
df-set send-icmp |
[df-set] drop |
[df-set] ipv4 |
[df-set] ipv6
}
```

Parameter	Description
df-set send-icmp	Enables sending of ICMP unreachable messages for inbound fragmented packets, and disallows overriding the Don't Fragment bit.
[**df-set**] **drop**	Drops inbound fragmented packets. The **df-set** option disallows override of the Don't Fragment bit.
[**df-set**] **ipv4**	Enables fragmentation support for inbound IPv4 packets. The **df-set** option disallows override of the Don't Fragment bit.
[**df-set**] **ipv6**	Enables fragmentation support for inbound IPv6 packets. The **df-set** option disallows override of the Don't Fragment bit.

Default By default, fragmentation for IPv6 tunnel packets is enabled but fragmentation of IPv4 packets within the tunnel is disabled. Override of the Don't Fragment bit is enabled.

Mode Configuration mode

cgnv6 ds-lite fragmentation outbound

Description Configure fragmentation support for outbound packets.

Syntax

```
[no] cgnv6 ds-lite fragmentation outbound
{
df-set send-icmp |
[df-set] drop |
[df-set] ipv4 |
[df-set] send-icmpv6
}
```

Parameter	Description
df-set send-icmp	Enables sending of ICMP unreachable messages for outbound IPv4 fragmented packets, and disallows

Parameter	Description
	overriding the Don't Fragment bit.
[df-set] drop	Drops outbound fragmented packets. The df-set option disallows override of the Don't Fragment bit.
[df-set] ipv4	Enables fragmentation support for outbound IPv4 packets. The df-set option disallows override of the Don't Fragment bit.
[df-set] send-icmpv6	Enables sending of ICMPv6 unreachable messages for outbound IPv6 fragmented packets, and disallows overriding the Don't Fragment bit. The df-set option disallows override of the Don't Fragment bit.

Default By default, fragmentation for IPv6 tunnel packets is enabled but fragmentation of IPv4 packets within the tunnel is disabled. Override of the Don't Fragment bit is enabled.

Mode Configuration mode

cgnv6 ds-lite icmp

Description Send ICMP Destination Unreachable messages when there are no protocol ports available for NAT mappings, or when a a user quota is exceeded.

Syntax

```
[no] cgnv6 ds-lite icmp
{send-on-port-unavailable | send-on-user-quota-exceeded}
{host-unreachable | admin-filtered | disable}
```

Parameter	Description
send-on-port-unavailable	Sends ICMP Destination Unreachable message when there are no protocol ports available for NAT mappings.
send-on-user-	Sends ICMP Destination Unreachable message

Parameter	Description
quota-exceeded	when a a user quota is exceeded.
host-unreachable	Sends code type 3, code 1 for IPv4, and type 1 code 3 for IPv6.
admin-filtered	Sends code type 3, code 13, administratively filtered.
disable	Disable ICMP Unreachable messages for the specified event.

Default The default for **send-on-port-unavailable is disable**. The default for **send-on-user-quota-exceeded** is **admin-filtered**.

Mode Configuration mode

cgnv6 ds-lite inside source class-list

Description Bind a class list for use with DS-Lite.

Syntax

```
[no] cgnv6 ds-lite inside source class-list list-name
```

Replace *list-name* with the name of the class list.

Default None

Mode Configuration mode

cgnv6 ds-lite ip-checksum-error

Description Configure handling of IP checksum errors in DS-Lite tunneled IP traffic.

Syntax

```
[no] cgnv6 ds-lite ip-checksum-error {fix | drop}
```

Parameter	Description
fix	Fixes the checksum and forwards the traffic.
drop	Drops the traffic.

Default **drop**

Mode Configuration mode

Usage IP checksum handling applies to IPv4 packets encapsulated within a DS-Lite tunnel.

This command applies only to IP traffic that is encapsulated inside a DS-Lite tunnel. The ACOS device always drops other IPv4 traffic that has an invalid checksum.

cgnv6 ds-lite l4-checksum-error

Description Configure handling of Layer 4 checksum errors in DS-Lite tunneled IP traffic.

Syntax

```
[no] cgnv6 ds-lite l4-checksum-error {fix | drop | propagate}
```

Default **propagate**

Mode Configuration mode

Usage Layer 4 checksum handling applies to TCP, UDP, and ICMP packets encapsulated within a DS-Lite tunnel.

This command applies only to IP traffic that is encapsulated inside a DS-Lite tunnel. The ACOS device always drops other IPv4 traffic that has an invalid checksum.

cgnv6 ds-lite port-reservation

Description Configure static mappings for a range of protocol ports for an IPv4 address

Syntax

```
[no] cgnv6 ds-lite port-reservation inside
ipv6-tunnel-source ipv6-tunnel-destination
ipv4-inside-addr inside-start-port inside-end-port
nat nat-ipaddr nat-start-portnum nat-end-portnum
```

Parameter	Description
ipv6-tunnel-source	Inside client's tunnel source IPv6 address.
ipv6-tunnel-destination	Inside client's tunnel destination IPv6 address.
ipv4-inside-addr	Client IPv4 address.

Parameter	Description
inside-start-portnum	Beginning Layer 4 protocol port number in the port range to be mapped.
inside-end-port	Ending Layer 4 protocol port number in the port range to be mapped.
nat *nat-ipaddr*	Public IPv4 address to map to the client IPv4 address.
nat-start-portnum	Beginning Layer 4 protocol port number to map to the inside port range.
nat-end-portnum	Ending Layer 4 protocol port number to map to the inside port range.

Default None

Mode Configuration mode

cgnv6 ds-lite tcp mss-clamp

Description Configure TCP maximum segment size (MSS) clamping. MSS clamping checks the TCP MSS value in packets from IPv4 clients and, if necessary, changes it before sending the NATted request to the server.

Syntax

```
[no] cgnv6 ds-lite tcp mss-clamp
{fixed n | none | subtract s [min n]}
```

Parameter	Description
fixed *n*	Changes the MSS to the length you specify.
none	Does not change the MSS value.
subtract *s* [**min** *n*]	Reduces the MSS if it is longer than the specified number of bytes. This option sets the MSS based on the following calculations: • If MSS minus S is greater than N, subtract S from the MSS. • If MSS minus S is less than or equal to N, set the MSS to N.

Parameter	Description
	The subtract method of MSS clamping is used by default, with the following values: • `S = 40 bytes` • `N = 416 bytes` Using these values, the default MSS clamping calculations are as follows: • If MSS minus 40 is greater than 416, subtract 40 from the MSS. • If MSS minus 40 is less than or equal to 416, set the MSS to 416.

Default The **`subtract`** option is used by default.

Mode Configuration mode

cgnv6 ds-lite tcp reset-on-error

Description Send TCP resets to DS-Lite clients in response to invalid TCP packets from the inside network.

Syntax `[no] cgnv6 ds-lite tcp reset-on-error outbound disable`

Default Enabled

Mode Configuration mode

cgnv6 ds-lite user-quota-prefix-length

Description Assign a user quota to all users of a specific DS-Lite prefix.

Syntax `[no] cgnv6 ds-lite user-quota-prefix-length` *num*

Default 128

Mode Configuration mode

Usage

You can apply a user quota prefix length on a global level or per LSN LID basis. The user quota prefix length set for an LSN LID overrides the global configuration value.

If the user quota prefix length is broader than the subnet to which the LSN LID is bound, the user quota may not be enforced. For the command **`show cgnv6 ds-lite user-quota-sessions`**, if a user quota prefix length is configured, only the prefix quota is displayed. If the prefix quota is not set, only the user quota session is displayed.

Port Control Protocol Commands

ACOS implements Port Control Protocol (PCP) fully compliant with RFC6887, and it supports port mapping allocations for the following CGN features: LSN (NAT44), Dual-Stack Lite (DS-Lite), NAT64, and Fixed-NAT LSN/DS-Lite/NAT64.

ACOS supports the following important PCP features. However, this list is not all-inclusive:

- PCP MAP Opcode
- PCP PEER Opcode
- PCP ANNOUNCE Opcode
- THIRD_PARTY option for PCP MAP/PEER
- PREFER_FAILURE option for PCP MAP
- FILTER option for PCP MAP
- Validating “nonce” in PCP MAP request

cgnv6 pcp default-template

Description Specify the Port Control Protocol (PCP) template to use as the set of default PCP settings.

Syntax

```
[no] cgnv6 pcp default-template template-name
```

Replace *template-name* with the name of the PCP template.

Default PCP is disabled by default. To enable it, configure a PCP template, then activate it on a global basis using the **cgnv6 pcp default-template** command.

Mode Configuration mode

Usage When PCP is enabled, the ACOS device acts as a PCP server for Large Scale NAT (LSN) clients (PCP clients). The ACOS device parses incoming UDP packets arriving on the PCP port, extracts the relevant information, and creates or refreshes the IPv4-IPv4 mapping as requested by the PCP client. The ACOS device then sends a PCP

response message back to the PCP client. The mapping created for the client is an implicit dynamic mapping.

Related Commands:

- cgnv6 template pcp

cgnv6 template pcp

Description Configure a template to set Port Control Protocol (PCP) options.

Syntax

```
[no] cgnv6 template pcp template-name
```

Replace *template-name* with the name of the template, 1-31 characters.

This command changes the CLI to the configuration level for the template, where the following commands are available.

(The other commands are common to all CLI configuration levels.)

Command	Description
[no] allow-third-party-from-lan	Enables support for the third-party option in MAP requests received on the LAN. This option instructs the ACOS device to use the address specified in the MAP request, instead of the source address of the request packet, as the internal address for the mapping. By default, this option is disabled.
[no] allow-third-party-from-wan	Enables support for the third-party option in MAP requests received on the WAN. This option instructs the ACOS device to use the address specified in the MAP request, instead of the source address of the request packet, as the internal address for the mapping. By default, this option is disabled.
[no] check-client-nonce	Enable validation of the PCP MAP NONCE. By default, this option is disabled.
[no] disable-map-filter	Disable the process to FILTER in PCP MAP. By default, this option is enabled.
[no] disable-	Enable or disable the process for

Command	Description
opcode *option*	MAP/PEER/ANNOUNCE Opcodes. Available options are: • **announce** • **map** • **peer** All three options are enabled by default.
[**no**] **mapping-lifetime**	Specifies the maximum lifetime of PCP mappings. Available options are: • **maximum** – You can specify 2 -1440 minutes. The default is 1440 minutes. • **minimum** – You can specify 2 -1440 minutes. The default is 2 minutes.
[**no**] **pcp-server-port** *portnum*	Specifies the UDP destination port for PCP, 1024-65535. The default is 5351.
[**no**] **send-unsolicited-announce** {**source-ip** *ipv4addr* | **source-ipv6** *ipv6addr*}	Allows the ACOS device to send an unsolicited announce packet when the ACOS device reboots or reloads, or following VRRP-A failover. By default, the configuration is disabled.

Default PCP disabled by default. To enable it, use this command to configure a PCP template, then use the **cgnv6 pcp default-template** command to activate it (cgnv6 pcp default-template).

Mode Configuration mode

Usage The current release supports PCP only for IPv4-IPv4 mappings for LSN clients. PCP is not supported for IPv6 mappings or for other IPv6 migration features (NAT64, DS-Lite, and so on).

ACOS supports RFC 6887- compliant Port Control Protocol (draft 29). For more information, see RFC 6887. Draft versions 12 and 13 are no longer supported.

Logging Template Commands

This section describes the configuration commands for CGN logging templates. Logging templates are applicable to IPv6 migration features.

cgnv6 template logging

Description Configures a template for external logging of LSN / DS-Lite traffic events.

Syntax

```
[no] cgnv6 template logging template-name
```

This command changes the CLI to the configuration level for the specified NAT logging template, where the following command is available.

(The other commands are common to all CLI configuration levels.)

Command	Description
[no] batched-logging-disable	Disables batching of multiple log messages in the same external logging packet. When this option is enabled, only a single log message is placed in each packet.
[no] custom *options*	Configures custom LSN log strings. • **custom header use-syslog-header** – Adds a syslog header to each message. (Disabled by default. By default, no header is included.) • **custom message** *type string* – Customizes a logging string. The *type* can be one of the following: ○ **fixed-nat-allocated** ○ **fixed-nat-freed** ○ **fixed-nat-interim-update**

Command	Description
	○ **http-request-got** ○ **port-allocated** ○ **port-batch-allocated** ○ **port-batch-freed** ○ **port-batch-v2-allocated** ○ **port-batch-v2-freed** ○ **port-batch-v2-interim-update** ○ **port-freed** ○ **session-created** ○ **session-deleted** ○ `message-string` - Specify an arbitrary log message string (1-255 characters) for custom logging by including only relevant events and fields. You can also include event-specific details such as session start time, session duration, and more by using certain predefined keywords. These keywords must be enclosed in dollar signs ($). For the keyword list, see Custom Format Keywords. • **customtime-stamp-format**– Customizes the time stamp format to use in the message strings. The default format is <%Y><%m><%d><%H%M%S>, where <%m> displays the month numerically. You can also set the time stamp format as "<%Y> <%o> <%d> <%H:%M:%S>", where <%o> represents the month displayed in three-letter alphabets. The mapping between the numerical months and their corresponding three-letter month is as follows: 1 - Jan, 2 - Feb, 3 - Mar, 4 - Apr, 5 - May, 6 - Jun, 7 - Jul, 8 - Aug, 9 - Sep, 10 - Oct, 11 - Nov, 12

Command	Description
	- Dec.
[no] **disable-log-by-destination**	Disables logging by specific protocol and destination port/range of ports. The following options are available: • **icmp** – disables logging for ICMP traffic • **ip** – configures a filter for IP entry • **ip6** – configures a filter for IPv6 entry • **others** – disables logging for other protocols • **tcp** – disables logging by destination TCP port • **udp** – disables logging by destination UDP port
[no] **enable-log-by-destination**	Enables logging by specific protocol, destination IP address, port, and range of ports. The following options are available: • **icmp** – enables logging for ICMP traffic • **ip** – configures a filter for IP entry • **ip6** – configures a filter for IPv6 entry • **others** – enables logging for other protocols • **tcp** – enables logging by destination TCP port • **udp** – enables logging by destination UDP port
[no] **facility** *facility-name*	Specifies the logging facility to use. For a list of available facilities, enter the following command: **facility ?**
[no] **format** *option*	Reduces the size of external traffic logs. You can enable one of the following data reduction options: • **binary** – Uses a unique A10 Binary Logging format to represent the log messages. • **compact** – Uses ASCII text format. It reduces the log size by using operational codes (“opcodes”)

Command	Description
	for event and protocol names, and by using hexadecimal representation for IPv4 addresses and port numbers. • **custom** – Uses an arbitrary custom logging format. • **default** – Uses ASCII text format for external log messages, with IP addresses and port numbers represented in decimal format. Likewise, the event and protocol names are spelled out. • **rfc5424** – Uses the format defined in RFC 5424, The Syslog Protocol. • **cef** – Uses the Common Event Format for logging. For more information, see "NAT Logging" topic of the IPv4-to-IPv6 Transition Solutions Guide. **NOTE:** RADIUS logging is only available in ASCII format.
[**no**] **include-destination**	Includes the destination IP addresses and protocol ports in NAT port mapping logs.
[**no**] **include-http***option*	Includes additional HTTP information in the log messages. • **cookie** [**max-length***num*] – Includes cookie information. • **file-extension** – Includes HTTP file extension. • **l4-session-info** – Includes TCP session information. • **method** – Includes the HTTP method; for example: GET or POST. • **referer** [**max-length** *num*] – Includes the information in the Referer header.

Command	Description
	• **request-number** – Includes the HTTP request number. • **user-agent** [**max-length** *num*] – Includes the information in the User-Agent header. • **header1** [**max-length** *num*],**header2** [**max-length** *num*],**header3** [**max-length** *num*]– Includes up to 3 additional headers. The **max-length** option specifies the maximum number of characters to include for each header. You can specify 100-1000. the default is 100.
[**no**] **include-inside-user-mac**	Inserts client MAC addresses into traffic logs.
[**no**] **include-partition-name**	Includes the ADP partition names in logs.
[**no**] **include-radius-attribute** {**framed-ipv6-prefix** **{prefix-length}**| **imei** | **imsi** | **msisdn** | **custom1** | **custom2** | **custom3** | **no-quote**}	Includes the client mobile number in Carrier Grade NAT (CGN) traffic logs. The ACOS device obtains the client mobile number by sending a RADIUS Accounting request to an external RADIUS server for the specified attribute. The attribute can be one of the following: • **framed-ipv6-prefix** – Include RADIUS attributes for the prefix. You must specify the **prefix-length** designated for the prefix. • **imei** – International Mobile Equipment Identity • **imsi** – International Mobile Subscriber Identity • **insert-if-not-existing**– Configure what string is to be inserted for custom RADIUS attributes. • **msisdn** – Mobile Station International ISDN

Command	Description
	Number • **custom1**, **custom2**, **custom3** – Additional attributes not covered by other options • **no-quote** - No quotation marks for RADIUS attributes in logs. With the exception of **no-quote** and **framed-ipv6-prefix**, under each of this attribute, the following options are available: • The **http-requests**option includes the mobile number in HTTP request logs. • The **port-mappings** option inserts the mobile number into port-mapping logs, Fixed-NAT user port logs (if enabled), and Port Batching logs (if enabled). • The **sessions** option includes the mobile number in session logs. • The **user-data** option enables the subscriber information to be included in the enhanced user tracking logs.
[**no**] **include-session-byte-count**	Includes the byte-count in session deletion logs.
[**no**] **log***option*	Enables logging for specific options. • **fixed-nat** { **http-requests** {**host** | **url**} | **port-mappings** {**both** | **creation**} | **sessions** | **user-ports** [**periodic** *days* **start-time** *hh*:*mm*] }

Command	Description
	Enables logging for Fixed-NAT. • **http-requests** {**host** | **url**} Enables logging of information from HTTP requests. **NOTE:** The maximum length of the **log http-requests host** option is 255. • **port-mappings** {**both** | **creation**} Logs Fixed-NAT port mappings. Use **both** to log both creation and deletion of NAT mappings; use **creation** to log creation of MAT mappings only. • **sessions** [**merged-style**] Logs Fixed-NAT session creation and deletion. The **merged-style** option merges creation and deletion of session logs to one. • **user-ports** [**periodic** *days* **start-time** *hh:mm*] Includes the port numbers assigned to clients. The **periodic** option specifies the Interval between log generation for Fixed-NAT port allocations. You can specify 1-30 days. The **start-time** option specifies the time at which to generate the first user activity log. This is the local system time on the ACOS device. • **http-requests** {**host** | **url**} Enables logging of information from HTTP requests. • **host** logs the hostname requested by the client. • **url** logs the URL requested by the client.

Command	Description
	• **port-mappings** {**creation** | **disable**} Enables logging of LSN port mapping events. The **creation** option logs Fixed-NAT session creation only. If you omit this option, session deletion also is logged. • **creation** Logs mapping creation only. • **disable** Disables logging for port mapping. • **port-overloading** Logs all port overloading sessions. • **sessions** [**merged-style**] Enables logging of data session events. **merged-style** merges creation and deletion of session logs to one. • **user-data** Enables the enhanced user tracking logs to be sent out to external syslog servers.
[**no**] **log-receiver radius secret** {*secret-string* | **encrypted**}	Enables use of RADIUS for external logging. • **secret-string** – The password required by the RADIUS server for authentication requests. • **encrypted** – The A10 reserved encrypted keyword. Do NOT use this option manually. **NOTE:** The "**no**" form of the command returns the logging method to its default, Syslog.
[**no**]	Specifies the precision of the timestamps in log

Command	Description
resolution	messages. • **seconds** – Log message timestamps are precise to within one whole second. • **10-milliseconds** – Log message timestamps are precise to within 1/100 second (10 milliseconds).
[**no**] **rfc-custom header use-alternate-timestamp**	Use the following timestamp format: *YYYY MMM DD HH:MM:SS* Enabling this option disables use of timestamps formatted in compliance with RFC 5424, The Syslog Protocol.
[**no**] **rfc-custom message** *feature type string*	Customizes log message strings for external logging. The feature can be one of the following: • **http-request-got** – Message strings for HTTP request logs. The message-string must be in the following format: "MSG-ID [STRUCTURED-DATA] MSG" • **lsn** – Message strings for CGN traffic. • **nat64** – Message strings for NAT64 traffic. • **ds-lite** – Message strings for DS-Lite traffic. • **sixrd-nat64** – Message strings for 6rd-NAT64 traffic. The type can be one of the following: • **fixed-nat-allocated** – Fixed-NAT allocated. • **fixed-nat-freed** – Fixed-NAT freed. • **port-allocated** – Port allocated. • **port-batch-allocated** – Port Batch allocated

Command	Description
	• **port-batch-freed** – Port Batch freed • **port-batch-v2-allocated** – Port Batch v2 allocated • **port-batch-v2-freed** – Port Batch v2 freed • **port-freed** – Port freed • **session-created** – Message strings for session creation. • **session-deleted** – Message strings for session deletion. **NOTE:** The **fixed-nat-allocated** and **fixed-nat-freed** message types apply only to feature types **lsn** and **nat64**. The *string* specifies the fields and text to use in the message strings. (For more information, see "RFC 5424 Header Support For External Logging" section in the IPv4-to-IPv6 Transition Solutions Guide.)
[**no**] **rule http-requests** *option*	Configures rules for HTTP request logging. You can set the following options: • **dest-port** *portnum* [**include-byte-count**] – Destination TCP port for which to log client requests. For example, to log client requests to port 80, enter the following command: **rule http-requests dest-port 80**. The **include-byte-count** option also adds the byte count to the log messages. • **disable-sequence-check** – Disables HTTP packet sequence check and don't drop out packets. HTTP sequence check is enabled by default. This HTTP sequence check is required for HTTP logging. If

Command	Description
	disabled, out-of-order HTTP requests will not be logged. • **include-all-headers** – Includes all configured headers even when they are absent in the HTTP request. • **log-every-http-request** – Logs every HTTP request in a client session. Without this option, only the first request in the session is logged. • **max-url-len** *max-number-of-characters* – Maximum number of characters logged for each URL string. You can specify 100-1000 characters. **NOTE:** Some limitations may apply.
[**no**] **rule port-mappings** [**interim-update** *minutes*]	Specifies the interim update interval in minutes. You can specify 15-120 minutes.
[**no**] **service-group** *group-name*	Specifies the service group for the external log servers.
[**no**] **severity** *severity-level*	Specifies the severity level to assign to LSN traffic logs generated using this template. You can enter the name or the number of a severity level. • **0 | emergency** • **1 | alert** • **2 | critical** • **3 | error**

Command	Description
	• **4 | warning** • **5 | notice** • **6 | informational** • **7 | debug**
[**no**] **source-address** {**ip** *ipv4addr* | **ipv6** *ipv6addr*}	Specifies the source IPv4 or IPv6 address to use as the source of log packets.
[**no**] **source-port** {*portnum* | **any**}	Specifies the source protocol port the ACOS device uses to send out log messages to the external log servers. • If the **any** option is configured, the ACOS device randomly selects a source-port for each logging packet. • The **source-port** command is only applicable to syslog over UDP, and does not apply to TCP traffic. With syslog over TCP traffic, the source port is determined by the ACOS device through Smart NAT. **NOTE:** This does not conflict with the real server port, which is the destination port of the logging packet.

Default There is no NAT logging template by default. When you configure one, the template options have the following default values:

- **batched-logging-disable** – disabled. Log messages are batched. Each external logging packet can contain more than one log message.
- **custom** – not set

- **facility** – local0
- **format** – default (ASCII)
- **include-destination** – disabled
- **include-http** – not set
- **include-inside-user-mac** – not set
- **include-partition-name** – not set
- **include-radius-attribute** – not set
- **log fixed-nat** – all options disabled
- **log fixed-nat-user-ports** – disabled
- **log http-requests** – disabled
- **log port-mappings** – Both creation and deletion of mappings are logged.
- **log port-overloading** – disabled
- **log sessions** – disabled
- **log-receiver** – not set
- **resolution** – seconds
- **rfc-custom** – The default message formats are used, if RFC 5424 format is enabled. (For more information, see IPv4-to-IPv6 Transition Solutions Guide.)
- **rule** – Rules for HTTP request logging have the following defaults:
  - **dest-port** – not set
  - **log-every-http-request** – disabled; only the first request of the session is logged
  - **max-url-len** – 100
- **service-group** – not set
- **severity** – 7 (debugging)
- **source-address** – IP address of the Ethernet data interface out which the log packet is sent.
- **source-port** – 514 (for UDP only)

Mode Configuration mode

Usage

The template does not take effect until you set it as the default LSN / DS-Lite logging template or assign it to individual LSN / DS-Lite pools.

- Use cgnv6 lsn logging default-template to set the template as the default LSN / DS-Lite logging template.
- Use cgnv6 lsn logging pool to assign the template to an LSN / DS-Lite pool.

Maximum URL Length for HTTP Request Logging

The maximum number of URL characters that can be logged depends on the log format settings, as listed in the table below:

Logging Option	Maximum URL Characters Logged
Default data format (ASCII)	1000
Compact data format	
RFC 5424 format	
Binary data format	253
Logging to RADIUS	247

Additional characters are truncated from the right side of the URL string.

The custom format allows you to include event-specific details such as session start time, session duration, and more by specifying certain predefined keywords. The following tables list the keywords that can be included in the custom logging format:

Keywords for **session-creation** event:

Keyword	Description
$rule-name$	**Rule used in the session.**
$proto-name$	**Protocol used in the session.**
$proto-	**Protocol number used in the session.**

Keyword	Description
num$	
$fwd-tuple-type$	Forward tuple type used in the session.
$fwd-tun-nel$	Forward tuple tunnel IP used in the session.
$fwd-src-ip$	Forward tuple source IP address of the session.
$fwd-src-port$	Forward tuple source port number of the session.
$fwd-dst-tun-nel$	Forward tuple destination tunnel used in the session.
$fwd-dst-ip$	Forward tuple destination IP address of the session.
$fwd-dst-port$	Forward tuple destination port number of the session.
$rev-tuple-type$	Reverse tuple type used in the session.
$rev-tun-nel$	Reverse tuple tunnel IP address of the session.
$rev-src-ip$	Reverse tuple source IP address of the session.
$rev-src-port$	Reverse tuple source port number of the session.
$rev-dst-tun-nel$	Reverse tuple destination tunnel used in the session.

Keyword	Description
$rev-dst-ip$	**Reverse tuple destination IP address of the session.**
$rev-dst-port$	**Reverse tuple destination port number of the session.**
$sesn-start-time$	**Start time of the session.**
$sesn-start-time-epoch$	**Epoch start time of the session.**
$radius-msisdn$	**RADIUS attribute: MSISDN**
$radius-imei$	**RADIUS attribute: IMEI**
$radius-imsi$	**RADIUS attribute: IMSI**
$radius-ctm1$	**RADIUS attribute: Custom1**
$radius-ctm2$	**RADIUS attribute: Custom2**
$radius-ctm3$	**RADIUS attribute: Custom3**
$radius-ctm4$	RADIUS attribute: Custom4
$radius-ctm5$	RADIUS attribute: Custom5
$radius-ctm6$	RADIUS attribute: Custom6

Keywords for **session-delete** event:

Keyword	Description
$rule-name$	Rule used in the session.
$proto-name$	Protocol used in the session.
$proto-num$	Protocol number used in the session.
$fwd-tuple-type$	Forward tuple type used in the session.
$fwd-tun-nel$	Forward tuple tunnel IP used in the session.
$fwd-src-ip$	Forward tuple source IP address of the session.
$fwd-src-port$	Forward tuple source port number of the session.
$fwd-dst-tun-nel$	Forward tuple destination tunnel used in the session.
$fwd-dst-ip$	Forward tuple destination IP address of the session.
$fwd-dst-port$	Forward tuple destination port number of the session.
$rev-tuple-type$	Reverse tuple type used in the session.
$rev-tun-nel$	Reverse tuple tunnel IP address of the session.
$rev-src-ip$	Reverse tuple source IP address of the session.
$rev-	Reverse tuple source port number of the session.

Keyword	Description
src-port$	
$rev-dst-tunnel$	Reverse tuple destination tunnel used in the session.
$rev-dst-ip$	Reverse tuple destination IP address of the session.
$rev-dst-port$	Reverse tuple destination port number of the session.
$req-byte$	Request byte count of the session.
$rsp-byte$	Response byte count of the session.
$sesn-dur$	Duration of the session.
$sesn-fwd-byte$	Forward byte count of the session.
$sesn-rev-byte$	Reverse byte count of the session.
$sesn-start-time$	Start time of the session.
$sesn-start-time-epoch$	Epoch start time of the session.
$sesn-end-time$	End time of the session.

Keyword	Description
$sesn-end-time-epoch$	**Epoch end time of the session.**
$radius-msisdn$	**RADIUS attribute: MSISDN**
$radius-imei$	**RADIUS attribute: IMEI**
$radius-imsi$	**RADIUS attribute: IMSI**
$radius-ctm1$	**RADIUS attribute: Custom1**
$radius-ctm2$	**RADIUS attribute: Custom2**
$radius-ctm3$	**RADIUS attribute: Custom3**
$radius-ctm4$	RADIUS attribute: Custom4
$radius-ctm5$	RADIUS attribute: Custom5
$radius-ctm6$	RADIUS attribute: Custom6

Example

The following commands configure external logging for LSN / DS-Lite traffic events, using the same template for all LSN / DS-Lite pools:

```
ACOS(config)# cgnv6 server syslog1 192.168.1.100
ACOS(config-real server)# port 514 udp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# cgnv6 service-group syslog udp
ACOS(config-cgnv6 svc group)# member syslog1 514
ACOS(config-cgnv6 svc group)# exit
ACOS(config)# cgnv6 template logging lsn_logging
ACOS(config-logging:lsn_logging)# log port-mappings creation
```

```
ACOS(config-logging:lsn_logging)# service-group syslog
ACOS(config-logging:lsn_logging)# exit
ACOS(config)# cgnv6 lsn logging default-template lsn_logging
```

Example The following commands configure the time stamp to display the month in the three-letter alphabet in the custom log message:

```
ACOS(config)# cgnv6 template logging temp
ACOS(config-logging:temp)# custom time-stamp-format "<%Y> <%o>
<%d> <%H:%M:%S>"
```

Example The following commands disable the TCP port and UDP port for logging:

```
ACOS(config)# cgnv6 template logging temp
ACOS(config-logging:temp)# disable-log-by-destination
ACOS(config-logging:temp-filter)# tcp port 90
ACOS(config-logging:temp-filter)# udp port 53
ACOS(config-logging:temp-filter)# icmp
```

Example The following commands disable the IPv4 address for logging:

```
ACOS(config)# cgnv6 template logging temp
ACOS(config-logging:temp)# disable-log-by-destination
ACOS(config-logging:temp-filter)# ip 20.1.0.1/32
ACOS(config-logging:temp-filter-ip)# udp port 5678
ACOS(config-logging:temp-filter-ip)# tcp port 80
ACOS(config-logging:temp-filter-ip)# icmp
```

Example The following commands enable the TCP port and UDP port for logging:

```
ACOS(config)# cgnv6 template logging temp
ACOS(config-logging:temp)# enable-log-by-destination
ACOS(config-logging:temp-filter)# tcp port 1000
ACOS(config-logging:temp-filter)# udp port 5678
ACOS(config-logging:temp-filter)# icmp
```

Example The following commands enable the IPv4 address for logging:

```
ACOS(config)# cgnv6 template logging temp
ACOS(config-logging:temp)# enable-log-by-destination
ACOS(config-logging:temp-filter)# ip 20.1.0.1/32
ACOS(config-logging:temp-filter-ip)# udp port 5678
ACOS(config-logging:temp-filter-ip)# tcp port 80
ACOS(config-logging:temp-filter-ip)# icmp
```

cgnv6 server

Description Configure a server for external logging.

Syntax

```
[no] cgnv6 server server-name ipaddr
```

Parameter	Description
server-name	Server name, 1-31 characters.
ipaddr	IP address of the server in either IPv4 or IPv6 format. The address is required only if you are creating a new server.

This command changes the CLI to the configuration level for the specified service-group, where the following command is available:

Command	Description
disable	Disables the server.
enable	Enables the server.
[**no**] **health-check** [*monitor-name*]	Enables health monitoring of the server. The *monitor-name* specifies the name of a configured health monitor. If you omit this command or you enter it without the *monitor-name* option, the default Layer 3 (ICMP) health monitor is used.
[**no**] **health-check-disable**	Disables health monitoring of the server.
[**no**] **health-check-follow-port** *portnum* {**tcp** | **udp**}	Specifies the specific port to follow for health status.
[**no**] **port** *port-num* {**tcp** | **udp**}	Specifies the TCP or UDP port on which the server listens for log traffic. **disable** | **enable** Disables or re-enables the port.

Command	Description
	[no] **health-check** [*monitor-name*] Enables health monitoring of the port. The monitor-name option specifies the name of a configured health monitor. If you omit the **health-check** command or you enter it without the monitor-name option, the default UDP health monitor is used. [no] **health-check-disable** Disables health monitoring of the port.

Default There is no default logging server configuration.

Mode Configuration mode

Usage The normal form of the **cgnv6 server** command creates a new or edits an existing real server. The CLI changes to the configuration level for the server.

The "no" form of this command removes an existing real server.

The IP address of the server can be in either IPv4 or IPv6 format. ACOS supports both address formats.

Default Default Health Monitoring

The following health monitors are enabled by default.

- ICMP – Server health check. Every 5 seconds, the ACOS device sends an ICMP echo request (ping) addressed to the server's IP address. The server passes the health check if it sends an echo reply to the ACOS device. If the server does not reply after the fourth attempt (the first attempt followed by 3 retries), the ACOS device sets the server state to DOWN.
- TCP – Every 5 seconds, the ACOS device sends a connection request (TCP SYN) to the specified TCP port on the server. The port passes the health check if it replies to the ACOS device by sending

a TCP SYN ACK. If the port does not reply after the fourth attempt, the ACOS device sets the port state to DOWN.

- UDP – Protocol port health check. Every 5 seconds, the ACOS device sends a packet with a valid UDP header and a garbage payload to the UDP port. The port passes the health check if the server either does not reply, or replies with any type of packet except an ICMP Error message.

cgnv6 service-group

Description Configure a service group, which is a pool of one or more servers.

Syntax

```
[no] cgnv6 service-group group-name {tcp | udp}
```

Replace *group-name* with the name of the group, 1-31 characters.

This command changes the CLI to the configuration level for the specified service-group, where the following command is available:

NOTE: The other configuration commands at this level are not applicable to logging.

Command	Description
[no] **health-check** [*monitor-name*]	Enables health monitoring of the service group. The **monitor-name** specifies the name of a configured health monitor.
[no] **member** *server-name portnum*	Adds the external log server and port to the service group.

Default There are no service groups configured by default.

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing service group. The CLI changes to the configuration level for the service group.

Fixed-NAT Command

This section describes the configuration command for Fixed-NAT.

NOTE: For Fixed-NAT, use of a NAT64 prefix with mapping to a class list is not supported.

cgnv6 ecmp 4-tuple-hash

Description Enable ECMP route and link load balancing to support 4-tuple hashing based on Source IP, Source Port, Destination IP, and Destination Port.

Syntax

```
[no] cgnv6 ecmp 4-tuple-hash
```

Mode Configuration mode

Usage This feature is enhanced to support 4-tuple hashing for UDP/TCP/ICMP for Static-NAT and LW-4o6 technologies, in addition to the previously supported UDP/TCP for DSLite, LSN, Fixed-NAT, NAT64, and Gi/SGi-FW transparent sessions.

Example The following shows how to enable ECMP 4-tuple hashing:.

```
ACOS(config)#  cgnv6 ecmp 4-tuple-hash
```

cgnv6 lsn alg

Description Disables or re-enables Application Level Gateway (ALG) support for LSN and Fixed-NAT.

Syntax

```
[no] cgnv6 lsn alg
{dns |esp | ftp | h323 | mgcp | pptp | rtp-stun-timeout | rtsp
| sip | tftp}
{enable | disable}
```

Parameter	Description
dns	Disables ALG support for Domain Name System (DNS).
esp	Enables or disables ALG support for Encapsulating Security Payload (ESP).

Parameter	Description
ftp	Enables or disables ALG support for File Transfer Protocol (FTP).
h323	Enables or disables ALG support H323 standard.
mgcp	Enables or disables ALG support for Media Gateway Control Protocol (MGCP).
pptp	Enables or disables ALG support for Point-to-Point Tunneling Protocol (PPTP).
rtp-stun-timeout	Changes the RTP/RTCP Session Traversal Utilities for NAT (STUN) timeout for the RTP/RTCP sessions created by SIP, MGCP, and H323. The timeout duration is 2 to 10 minutes. The default timeout value is 5 minutes.
rtsp	Enables or disables ALG support for Real Time Streaming Protocol (RTSP).
sip	Enables or disables ALG support for Session Initiation Protocol (SIP).
tftp	Enables or disables ALG support for Trivial File Transfer Protocol (TFTP).

Default ALG support for FTP is enabled by default. ALG support for the other protocols is disabled by default.

Mode Configuration mode

cgnv6 fixed-nat create-port-mapping-file

Description Creates a port mapping file.

Syntax

```
[no] cgnv6 fixed-nat create-port-mapping-file
```

Default Not set

Mode Configuration mode

Example The following is an example of the command

```
ACOS(config)# cgnv6 fixed-nat create-port-mapping-file
```

cgnv6 fixed-nat port-mapping-files-count

Description Configures the number of old port-mapping files to retain.

Syntax

```
[no] cgnv6 fixed-nat port-mapping-files-count
```

Default Not set

Mode Configuration mode

Example The following is an example of the command

```
ACOS(config)# cgnv6 fixed-nat create-port-mapping-files-count
1
```

cgnv6 fixed-nat inside

Description Configures Fixed NAT inside users using IPv4 or IPv6 inside user address.

Syntax

```
[no] cgnv6 fixed-nat  inside
ip-list list-name  nat  ip-list  list-name {dest-rule-list |
dynamic-pool-size | method | offset | ports-per-user |
respond-to-user-mac | session-quota | usable-nat-ports | vrid}
```

This scenario configures Fixed NAT inside users with an IP-list.

The following is an example of this configuration:

```
ACOS(config)# cgnv6 fixed-nat inside ip-list TEMP nat ip-list
TEMP dest-rule-list TEMP dynamic-pool-size 0 method use-all-
nat-ips offset random ports-per-user 1 respond-to-user-mac
session-quota 1 usable-nat-ports 1024 1024 vrid 1
```

Syntax

```
[no] cgnv6 fixed-nat  inside
{ipv4-start-inside-addr ipv4-end-inside-addr  netmask  /nn
nat  start-nat-addr end-nat-addr  netmask  /nn {dest-rule-list
| dynamic-pool-size | method | offset | ports-per-user |
respond-to-user-mac | session-quota | usable-nat-ports | vrid}
```

This scenario configures FIXED NAT inside users with NAT start and end addresses.

The following is an example of this configuration:

```
ACOS(config)# cgnv6 fixed-nat inside 1.1.1.1 1.1.1.1 netmask
/24 nat 1.1.1.1 1.1.1.1 netmask /24 dest-rule-list TEMP
dynamic-pool-size 0 method use-all-nat-ips offset random
ports-per-user 1 respond-to-user-mac session-quota 1 usable-
nat-ports 1024 1024 vrid 1
```

Syntax

```
[no] cgnv6 fixed-nat  inside
{ipv4-start-inside-addr ipv4-end-inside-addr  netmask  /nn
partition  partition-name  nat  ip-list  list-name  {dest-
rule-list | dynamic-pool-size | method | offset | ports-per-
user | respond-to-user-mac | session-quota | usable-nat-ports
| vrid}
```

This scenario configures FIXED NAT inside users with an IP-list within an inside user partition.

The following is an example of this configuration:

```
ACOS(config)# cgnv6 fixed-nat inside 1.1.1.1 1.1.1.1 netmask
/24 partition TEMP  nat ip-list TEMP dynamic-pool-size 0 dest-
rule-list TEMP method use-all-nat-ips offset random ports-per-
user 1 respond-to-user-mac session-quota 1 usable-nat-ports
1024 1024 vrid 1
```

Syntax

```
[no] cgnv6 fixed-nat  inside
{ipv4-start-inside-addr ipv4-end-inside-addr  netmask  /nn
partition partition-name nat start-nat-addr end-nat-addr
netmask  /nn {dest-rule-list | dynamic-pool-size | method |
offset | ports-per-user | respond-to-user-mac | session-quota
| usable-nat-ports | vrid}
```

This scenario configures FIXED NAT inside users with NAT start and end addresses within an inside user partition.

The following is an example of this configuration:

```
ACOS(config)# cgnv6 fixed-nat inside 1.1.1.1 1.1.1.1 netmask
/24 partition TEMP nat 1.1.1.1 1.1.1.1 netmask /24 dynamic-
pool-size 0 dest-rule-list TEMP method use-all-nat-ips offset
random ports-per-user 1 respond-to-user-mac session-quota 1
usable-nat-ports 1024 1024 vrid 1
```

Parameter	Description
inside	IP address range(s) of inside clients.

Parameter	Description
options	To specify a single range: • *start-inside-ipaddr* – Beginning (lowest-numbered) inside client address. • *end-inside-ipaddr* – Ending (highest-numbered) inside client address. • **netmask** – Network mask, in the applicable format: ◦ IPv4 – **/***mask-length* or *ipaddr* ◦ IPv6 – *mask-length*
nat *options*	To specify a single range: • *start-nat-ipaddr* – Beginning (lowest-numbered) NAT address. • *end-nat-ipaddr* – Ending (highest-numbered) NAT address. To specify multiple ranges: • **ip-list** *list-name* – Name of a configured IP list.
partition *options*	Configures settings for inside user partition.
dest-rule-list *name*	Binds destination-based rule-list.
dynamic-pool-size *num*	Number of protocol ports on each NAT address to set aside for use by clients who run out of their reserved ports.
method {**use-all-nat-ips** | **use-least-nat-ips**}	Method for IP allocation. • **use-all-nat-ips**—Inside client IP addresses can be allocated with the intent to use all of the available NAT IP addresses. This new algorithm ensures that all NAT IP addresses are used, with little room for any unused NAT IP addresses.

Parameter	Description
	• **use-least-nat-ips**—Inside client IP addresses can be allocated to NAT addresses with the goal of minimizing the use of available public NAT IP Addresses. This is the current behavior. This configuration method may result in some unused NAT IP addresses.
offset {**random** | *offset-value*}	Allocation offset. (For more information, see the IPv6 Migration Logging Guide.)
ports-per-user *num*	Number of protocol ports to allocate to each new client. You can specify 1-64512.
respond-to-user-mac	Enables MAC-based nexthop routing for Fixed-NAT. The next route hop is based on the MAC address of the inside client's request. The ACOS device uses the MAC address, instead of the route table, to select the next hop for the reply. Replies that are sent to the client use the same route hop on which the request was received.
session-quota *quota-num*	Maximum number of sessions that can be created for a given client. You can specify 1-2147483647.
usable-nat-ports *starting-port ending-port*	Range of protocol ports that can be allocated to clients. You can specify 1024-65535.
vrid *vrid*	Adds the Fixed-NAT addresses to a VRRP-A VRID for redundancy.

Default Not set

Mode Configuration mode

Stateless NAT46 Commands

This section describes the configuration commands for stateless NAT46. Stateless NAT46 enables IPv4 clients to reach IPv6 servers, without the need to maintain per-connection information on the ACOS device.

cgnv6 nat46-stateless fragmentation inbound

Description Change fragmentation support for inbound IPv6-to-IPv4 traffic.

Syntax

```
[no] cgnv6 nat46-stateless fragmentation inbound
{ipv4 | drop | send-icmpv6}
```

Parameter	Description
drop	IPv4 fragmentation is not allowed. Oversize packets are dropped. No ICMPv6 error message is sent.
ipv4	IPv4 fragmentation is allowed.
send-icmpv6	IPv4 fragmentation is not allowed. Oversize packets are dropped, and an ICMPv6 error message is sent.

Default **ipv4**

Mode Configuration mode

cgnv6 nat46-stateless fragmentation outbound

Description Change fragmentation support for outbound IPv4-to-IPv6 traffic.

Syntax

```
[no] cgnv6 nat46-stateless fragmentation outbound {df-set |
drop | ipv6}
```

Parameter	Description
df-set	Stateless NAT46 behavior if Don't Fragment (DF) bit is set for oversize packets. The default is send-icmp.
drop	IPv6 fragmentation is not allowed. Oversize packets are dropped. No ICMP error message is sent.
ipv6	IPv6 fragmentation is allowed.

Default **ipv6**

Mode Configuration mode

cgnv6 nat46-stateless fragmentation outbound df-set

Description Change fragmentation support for IPv4 packets that have the Don't Fragment bit set.

Syntax

```
[no] cgnv6 nat46-stateless fragmentation outbound df-set
{ipv6 | drop | send-icmp}
```

Parameter	Description
ipv6	IPv6 fragmentation is allowed.
drop	IPv6 fragmentation is not allowed. Oversize packets are dropped. No ICMP error message is sent.
send-icmp	IPv6 fragmentation is not allowed. Oversize packets are dropped, and an ICMP error message is sent.

Default **send-icmp**

Mode Configuration mode

cgnv6 nat46-stateless partition-prefix

Description Configure NAT46 prefix for L3V inter-partition NAT46 traffic.

Syntax

```
[no] cgnv6 nat46-stateless partition-prefix partition-name
ipv6-prefix [vrid vrid-num]
```

Default None

Mode Configuration mode

Usage Use this command to define a prefix that handles inter-partition NAT46 traffic going to L3V partitions. If a VRID is configured for a prefix, then only VRID-active ACOS devices will advertise this prefix.

cgnv6 nat46-stateless prefix

Description Configure a IPv6 prefix for stateless NAT46.

Syntax

```
[no] cgnv6 nat46-stateless prefix ipv6-prefix vrid vrid-num
```

Replace *ipv6-prefix* with the 96-bit prefix used as the higher-order bits of the client's IPv6 address and the *vrid-num* with the VRID configured for this prefix used for route advertisement.

Default None

Mode Configuration mode

Usage Stateless NAT46 translates an IPv4 client's address into an IPv6 address by combining the stateless NAT46 prefix configured on the ACOS device with the client's IPv4 address:

stateless_NAT46_prefix:client_IPv4_address

The stateless NAT46 prefix must be 96 bits long. This leaves 32 bits for the client's IPv4 address.

cgnv6 nat46-stateless static-dest-mapping

Description Configure static IPv4-IPv6 mappings for the IPv6 servers.

Syntax

```
[no] cgnv6 nat46-stateless static-dest-mapping ipv4addr
ipv6addr
[count num]
[shared | to-shared]
[vrid vrid]
```

Parameter	Description
ipv4addr	IPv4 server address to which IPv4 clients will send requests.
ipv6addr	Server's IPv6 address. Specify the lowest address in the range.
count *num*	Specifies how many mappings to create. The IPv4 and IPv6 addresses of each mapping are incremented by 1 over the previous mapping.
shared	This option is only available at the shared partition to share/expose this mapping with other partitions. This configuration shares/exposes the v4-address to all partitions. All traffic sent to this v4-address is initially handled as NAT46 traffic. If NAT46 fails, the traffic will

Parameter	Description
	then be handled as normal traffic.
to-shared	This option is only available at L3V partitions to send NAT-ed traffic through the shared partition. This mapping is used for inter-partition traffic. Any matching IPv4 traffic is translated to IPv6 traffic using the prefix defined in the shared partition (the partition-prefix configuration) and forward though the shared partition.
vrid *vrid*	Assigns the mappings to a VRRP-A VRID.

Default None

Mode Configuration mode

Usage Depending on the size of the system resources, the following lists the number of mappings supported:

- If the system memory is smaller than 16GB, then 1024 individual mappings are supported per partition.
- If the system memory is greater then 16GB, then 8K (8* 1024) mappings are supported per partition.

Specify only the first mapping in the range, and how many mappings to create. The ACOS device then automatically creates additional mappings, up to the quantity specified.

The IPv4 and IPv6 addresses for each additional mapping are incremented by 1 over the previous mapping. For example, suppose you specify the following mapping, and a quantity of 10:

- `20.0.0.1 -> 2001::1`

The ACOS device creates the following mappings:

- `20.0.0.1 -> 2001::1`
- `20.0.0.2 -> 2001::2`
- `20.0.0.3 -> 2001::3`
- `20.0.0.4 -> 2001::4`
- `20.0.0.5 -> 2001::5`

- 20.0.0.**6** -> 2001::**6**
- 20.0.0.**7** -> 2001::**7**
- 20.0.0.**8** -> 2001::**8**
- 20.0.0.**9** -> 2001::**9**
- 20.0.0.**10** -> 2001::**a**

cgnv6 nat46-stateless tcp mss-clamp

Description Configures TCP maximum segment size (MSS) clamping. MSS clamping checks the TCP MSS value in packets from IPv4 clients and, if necessary, changes the value before sending it out.

Syntax

```
[no] cgnv6 nat46-stateless tcp mss-clamp {none | fixed n |
subtract s [min n]}
```

Parameter	Description
fixed *n*	The fixed MSS value that you specify. The value can be 0 to 1420.
none	Does not change the MSS value.
subtract *s* [**min** *n*]	Reduces the MSS if it is greater than the specified number of bytes. • **subtract** - Value to subtract from the maximum MSS Clamping value. The value can be 0 to 1420. The default is 20. • **min** - Minimum value of the MSS Clamping in bytes. The value can be 0 to 1420. The default is 576-60-60. This option sets the MSS based on the following calculations: • If MSS minus S is greater than N, subtract S from the MSS. • If MSS minus S is less than or equal to N, set the MSS to N. The subtract method of MSS Clamping is used by default, with the following values:

Parameter	Description
	S = 40 bytes N = 576 bytes Using these values, the default MSS clamping calculations are as follows: • If MSS minus 40 is greater than 576, subtract 40 from the MSS. • If MSS minus 40 is less than or equal to 576, set the MSS to 576.

Default The **subtract**option is used by default.

Mode Configuration mode

Usage The TCP MSS value is the maximum amount of data a network host can accept in a single TCP segment. Use the ACOS CLI to set the maximum and minimum TCP MSS values and subtract the value from the configured maximum MSS. The minimum value is calculated as follows: `MSS Minimum = IP Header maximum – TCP Header maximum (TCP_MSS_MTU_MIN - TCP_MSS_IPH_MAX - TCP_MSS_TCPH_MAX).`

Example The following example shows how to configure the fixed value of 120 for MSS Clamping:

```
ACOS(config)# cgnv6 nat46-stateless tcp mss-clamp fixed 120
```

Example The following example shows how to configure the value of 100 to subtract from the TCP MSS and to configure the minimum value of 480 for MSS Clamping:

```
ACOS(config)# cgnv6 nat46-stateless tcp mss-clamp subtract 100
min 480
```

Lightweight 4over6 Commands

This section describes the global configuration commands for Lightweight 4over6 version of Dual-Stack Lite (DS-Lite).

Lightweight 4over6 enables the ACOS device to route traffic between an IPv4 client's IPv6 Customer Premises Equipment (CPE) and IPv4 servers. The IPv4 client's CPU performs NAT to assign a public IPv6 address to the client, then encapsulates the client's NATted IPv4 traffic in an IPv6 tunnel that is terminated on the ACOS device. Also see cgnv6 lw-4o6.

NOTE: The **cgnv6 lw-4o6** command can only be configured on the shared partition.

class-list (for lw4o6)

Description Configure an IP class list for use with Lightweight 4over6.

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a file.

Mode Configuration mode

Example Create a class-list of NAT IPv4 address prefixes to use for route redistribution, and apply the class-list to Lightweight 4over6.

```
ACOS(config)# class-list lw-4o6-nat-prefixes
ACOS(config-class list)# 15.10.10.171 /32
ACOS(config-class list)# 12.10.10.0 /24
```

cgnv6 lw-4o6

Description Configures LW-4over6.

Syntax

```
[no] cgnv6 lw-4o6 {binding-table | binding-table-validate |
hairpinning | health-check-gateway | icmp-inbound | inside-
src-access-list | nat-prefix-list | no-forward-match | no-
reverse-match | save-binding-table | use-binding-table}
```

See the following sections for each command.

Default Not set

Mode Global configuration mode

cgnv6 lw-4o6 binding-table

Description Configures a Lightweight 4over6 binding table directly on the ACOS device

Syntax `[no] cgnv6 lw-4o6 binding-table table-name`

This command changes the CLI to the configuration level for the specified class list, where the following command is available.

NOTE: This command can only be configured on the shared partition.

Command	Description
`[no] tunnel-address ipv6-address`	Specifies the IPv6 address of the tunnel endpoint address. This command creates an individual binding-table entry and changes the CLI to the configuration for that entry, where the following command is available: • `[no]nat-address ipv4-address` – Specifies the NAT IPv4 address for the given binding table entry. This command changes the CLI to the configuration level for the NAT address within that entry, where the following command is available: • `port num [tonum]` – Specifies the port range for the NAT address in the binding table entry. The `tunnel-endpoint-address` option is available to configure LW-4o6 IPIP Tunnel Endpoint Address. Using the “no” form of either the `nat-address` or `tunnel-address` command removes all entries associated with that specific NAT address or tunnel address respectively.

Default None

Mode Global configuration mode

Usage This command creates a Lightweight 4over6 binding table on the ACOS device, as well as all related entries for the binding table.

Example The following commands configure a LW-4o6 binding table “lw”:

```
ACOS(config)# cgnv6 lw-4o6 binding-table lw
ACOS(config-lw-4o6)# tunnel-address 2007:1:1:1::2007
ACOS(config-lw-4o6-ipv6)# nat-address 70.1.1.77
ACOS(config-lw-4o6-ipv6-nat)# port 1 to 65535 tunnel-endpoint-address 2007:1:1:1::2
```

Related Commands:

- cgnv6 lw-4o6 use-binding-table

cgnv6 lw-4o6 binding-table-validate

Description Checks and validates a Lw-4o6 binding-table for errors and log the error location and type into a file. It also checks an imported binding table and logs all the error entries into a file. If any error entries are found, a warning message indicates that errors are present in the validated binding table.

Syntax

```
cgnv6 lw-4o6 binding-table-validate table-name
```

Default None

Mode Global configuration mode

cgnv6 lw-4o6 fragmentation inbound

Description Configures fragmentation support for inbound packets.

Syntax

```
[no] cgnv6 lw-4o6 fragmentation inbound
{df-set | drop | ipv4 | ipv6}
```

Parameter	Description
df-set {**drop** | **ipv4** | **ipv6** |	The **df-set** option handles the packet when df-bit is set in the IPv4 header.

Parameter	Description
send-icmp}	The **send-icmp** option sends an ICMP Type 3 Code 4 (Destination unreachable - Fragmentation needed and DF set) to the source of the packet. This is the default option.
drop	Drops inbound packets that requires fragmentation.
ipv4	Enables fragmentation for IPv4 packets, of which fragments are then encapsulated in IPv6.
ipv6	Enables fragmentation for IPv4-in-IPv6 packets (after encapsulating IPv4 in IPv6). This is the default option. Fragmentation occurs on the outer header.

Default By default, for packets set with df-set, the default is **send-icmp**. For packets not set with df-set, the default is **ipv6**.

Mode Configuration mode

cgnv6 lw-4o6 fragmentation outbound

Description Configures fragmentation support for outbound packets.

Syntax

```
[no] cgnv6 lw-4o6 fragmentation outbound
{df-set | drop | ipv4 | send-icmpv6}
```

Parameter	Description
df-set {**drop** | **ipv4** | **send-icmp** | **send-icmpv6**}	The **df-set** option handles the packet when df-bit is set in the inner IPv4 header. The **send-icmp** option sends an ICMP Type 3 Code 4 (Destination unreachable - Fragmentation needed) in the tunnel to the source of the packet. This is the default option. The **send-icmpv6** option sends an

Parameter	Description
	ICMPv6 Type 2 Code 0 (Packet Too Big) to the tunnel source.
drop	Drops outbound packets that requires fragmentation.
ipv4	Enables fragmentation for IPv4 packets, after de-encapsulating the IPv4-in-IPv6 packet.
send-icmpv6	Enables sending of ICMPv6 Type 2 Code 0 (Packet Too Big) to the tunnel source.

Default By default, for packets set with df-set, the default is **send-icmp**. For packets not set with df-set, the default is **ipv4**.

Mode Configuration mode

cgnv6 lw-4o6 hairpinning

Description Configures hairpinning for Lightweight 4over6 clients.

Syntax

```
[no] cgnv6 lw-4o6 hairpinning
{
filter-all |
filter-none |
filter-self-ip |
filter-self-ip-port
}
```

Parameter	Description
filter-all	Drops all hairpinning traffic.
filter-none	Allows hairpinning without any restrictions.
filter-self-ip	Drops packets that have the same inside client IP address for both the source and destination.
filter-self-ip-port	Drops packets that have the same inside client IP address and protocol port number for both the source and destination. This option may be needed if double NAT is used.

Default **filter-none**

Mode Configuration mode

NOTE: This command can only be configured on the shared partition.

cgnv6 lw-4o6 health-check-gateway

Description Enforces gateway health monitoring for Lightweight 4over6. If any of the specified gateways fail a health check, ACOS will drop Lightweight 4over6 traffic and discontinue route redistribution:

Syntax

```
[no] cgnv6 lw-4o6 health-check-gateway ipaddr
```

Replace *ip-addr* with the IPv4 or IPv6 address of the gateway.

Example After you enable health monitoring for one or more gateways. ACOS will periodically check each gateway and drop Lightweight 4over6 traffic if any of the gateways are marked as down.

```
ACOS(config)# cgnv6 lw-4o6 health-check-gateway 9.9.9.173
ACOS(config)# cgnv6 lw-4o6 health-check-gateway 3201::172
```

NOTE: This command can only be configured on the shared partition.

cgnv6 lw-4o6 icmp-inbound

Description Configures handling of inbound IPv4 ICMP traffic for Lightweight 4over6 traffic. This applies to IPv4 traffic from the Internet fro sessions using Lightweight 4over6 bindings.

Syntax

```
[no] cgnv6 lw-4o6 icmp-inbound {drop | handle}
```

Parameter	Description
drop	Drops inbound ICMP traffic.
handle	Handles inbound ICMP traffic.

Default **handle**

Mode Configuration mode

NOTE: This command can only be configured on the shared partition.

Usage The feature applies only to inbound IPv4 traffic that is received on the Lightweight 4over6 inside NAT interface.

Related Commands:

- cgnv6 lw-4o6

cgnv6 lw-4o6 inside-src-access-list

Description Configure the Access List for Lightweight 4over6 inside clients.

Syntax

```
[no] cgnv6 lw-4o6 inside-src-access-list acl-num
```

Default None

Mode Configuration mode

Usage The feature applies an ACL to Lightweight 4over6 traffic.

NOTE: The acl-num option specifies the ACL number for the ACL to be applied to Lightweight 4over6 traffic.

cgnv6 lw-4o6 nat-prefix-list

Description Apply a class list to Lightweight 4over6 as the NAT Prefix List:

Syntax

```
[no] cgnv6 lw-4o6 nat-prefix-list class-list-name
```

Example The following example applies a class-list named “v-4o6” as the NAT Prefix List for Lightweight 4over6.

```
ACOS(config)# cgnv6 lw-4o6 nat-prefix-list v-4o6
```

NOTE: This command can only be configured on the shared partition.

cgnv6 lw-4o6 no-forward-match

Description Enables ICMPv6 Destination Unreachable messages (type 1, code 5) from the ACOS device to the client CPE.

Syntax

```
[no] cgnv6 lw-4o6 no-forward-match send-icmpv6
```

Default Disabled

Mode Configuration mode

NOTE: This command can only be configured on the shared partition.

Usage The feature applies only to outbound traffic on the Lightweight 4over6 outside NAT interface. (See cgnv6 lw-4o6.)

When this feature is enabled, the behavior is as follows:

- IPv6 tunnel address does not match any binding table entries
- Source IPv4 address matches a binding table entry, but the protocol port number does not match that entry
- Source IPv4 address and protocol port number match a binding table entry, but do not match the IPv6 tunnel address of that entry

cgnv6 lw-4o6 no-reverse-match

Description Enables ICMP Destination Unreachable messages (type 3, code 1) from the ACOS device to IPv4 servers.

Syntax

```
[no] cgnv6 lw-4o6 no-reverse-match send-icmp
```

Default Disabled

Mode Configuration mode

NOTE: This command can only be configured on the shared partition.

Usage The feature applies only to inbound IPv4 traffic that is received on the Lightweight 4over6 inside NAT interface.

When this feature is enabled, the behavior is as follows:

- If an inbound IPv4 packet's destination IPv4 address matches a binding-table entry but not the entry's protocol port(s), the ACOS device sends an ICMP message to the IPv4 packet's sender.
- If there is no binding-table match and the packet is not otherwise filtered out (for example, by an ACL on the inbound interface), the packet is forwarded at Layer 3.

Related Commands:

- cgnv6 lw-4o6

cgnv6 lw-4o6 save-binding-table

Description Saves the LW-4over6 binding table

Syntax

```
cgnv6 lw-4o6 save-binding-table
```

NOTE: This command can only be configured on the shared partition.

Mode Configuration mode

cgnv6 lw-4o6 use-binding-table

Description Activate a Lightweight 4over6 binding table.

Syntax

```
[no] cgnv6 lw-4o6 use-binding-table name
```

Replace *name* with the name of the binding table.

Default Disabled

Mode Configuration mode

NOTE: This command can only be configured on the shared partition.

Example Apply the Binding Table to Lightweight 4over6:

```
ACOS(config)# cgnv6 lw-4o6 use-binding-table bt1
```

MAP Commands

This section describes the global configuration commands for Mapping of Address and Port (MAP) technology.

cgnv6 map encapsulation domain

Description This command is used to enter the configuration level for a MAP-E domain on the ACOS device, whenever ACOS is used as a Border Relay in a MAP-E network.

Syntax

```
[no] cgnv6 map encapsulation domain domain-name
{basic-mapping-rule | description | format |
health-check-gateway | tunnel-endpoint-address}
```

Parameter	Description
basic-mapping-rule {**prefix-rule** *rule-name* | **rule-ipv4-address-port-settings**}	Configure the IPv6 address or prefix, and allows for MAP-E CPE to configure an IPv4 address based on the IPv6 prefix. **prefix-rule** – Configure the IPv6 and IPv4 prefix rule. For each prefix rule, there is the option to configure its own **rule-ipv4-address-port-settings**. If no such option is configured under the prefix rule, then the domain level **rule-ipv4-address-port-settings** is applied. **rule-ipv4-address-port-settings**: • **prefix-addr** – Each CE is assigned an IPv4 prefix. • **single-addr** – Each CE is assigned an IPv4 address. • **shared-addr** – Each CE is assigned a shared IPv4 address.
description *domain-name*	Create a description for the MAP-T domain

Parameter	Description
format {**draft-03**}	Configure the draft format for packet construction. By default, the packet is constructed/validated based on RFC format. This option changes the format to draft-03 format.
health-check-gateway {ipv4-addr | ipv6-addr | **withdraw-route**}	Configure a Health-check gateway for route withdrawn. **withdraw-route**: • **all-link-failure** – Withdraw routes on health-check failure of all IPv4 gateways or all IPv6 gateways • **any-link-failure** – Withdraw routes on health-check failure of any gateway (default)
tunnel-endpoint-address {ipv6-addr}	Configure the tunnel-endpoint-address as the destination address for traffic from the CPE. A single TEP can be used by multiple MAP domains.

Mode Global configuration mode.

This command can be used to create a new MAP-E domain on the ACOS device, or it can be used to enter the configuration level of an existing MAP-E domain in order to make changes to the domain configuration.

cgnv6 map encapsulation fragmentation inbound

Description Configures fragmentation support for inbound packets sent to the CPE.

Syntax

```
[no] cgnv6 map encapsulation fragmentation inbound
{df-set | drop | ipv4 | ipv6}
```

Parameter	Description
df-set {**drop** | **ipv4** | **ipv6** | **send-icmp**}	The **df-set** option handles packet when df-bit is set in the IPv4 header. The **send-icmp** option sends an ICMP Type 3

Parameter	Description
	Code 4 (Destination unreachable - Fragmentation needed and DF set) to the source of the packet. This is the default option.
drop	Drops inbound packets that requires fragmentation.
ipv4	Fragments the encapsulated IPv4 packet when sent to the CPE.
ipv6	Fragments the IPv6 tunnel packet when sent to the CPE. This is the default option. Fragmentation occurs on the outer header.

Default For packets set with **df-set**, the default is **send-icmp**. In other words, ICMP Type 3 Code 4 (Fragmentation Needed and DF Set) is sent. For packets not set with **df-set**, the default is **ipv6**.

Mode Configuration mode

cgnv6 map encapsulation fragmentation outbound

Description Configures fragmentation support for outbound packets sent to the server.

Syntax

```
[no] cgnv6 map encapsulation fragmentation outbound
{df-set  | drop | ipv4 | send-icmpv6}
```

Parameter	Description
df-set {**drop** | **ipv4** | **send-icmp** | **send-icmpv6**}	The **df-set** option handles the packet when df-bit is set in the inner IPv4 header. The **send-icmp** option sends an ICMP Type 3 Code 4 (Destination unreachable - Fragmentation needed) in the tunnel to the tunnel source if the outbound packet is to be fragmented. This is the default option. The **send-icmpv6** option sends an ICMPv6 Type 2 Code 0 (Packet Too Big) to the tunnel source if

Parameter	Description
	the outbound packet is to be fragmented to be sent to the server.
drop	Drops outbound packets that requires fragmentation.
ipv4	Fragments the encapsulated IPv4 packet when sent to the server.
send-icmpv6	Enables sending of ICMPv6 Type 2 Code 0 (Packet Too Big) to the tunnel source if the outbound packets is to be fragmented when sent to the server.

Default For packets set with **df-set**, the default is **send-icmp**. In other words, ICMP Type 3 Code 4 (Fragmentation Needed and DF Set) is sent. For packets not set with **df-set**, the default is **ipv4**.

Mode Configuration mode

cgnv6 map translation domain

Description This command is used to enter the configuration level for a MAP-T domain on the ACOS device, whenever ACOS is used as a Border Relay in a MAP-T network.

Syntax

```
[no] cgnv6 map translation domain domain-name
{basic-mapping-rule | default-mapping-rule | description |
health-check-gateway | mtu | tcp mss-clamp}
```

Parameter	Description
basic-mapping-rule {**prefix-rule** *rule-name* | **rule-ipv4-address-port-settings**}	Configure the IPv6 address or prefix, and allows for MAP-T CPE to configure an IPv4 address based on the IPv6 prefix. • **prefix-rule** – Configure the IPv6 and IPv4 prefix rule. • **rule-ipv4-address-port-settings**: • **prefix-addr** – Each CE is assigned an IPv4

Parameter	Description
	prefix. • **single-addr** – Each CE is assigned an IPv4 address. • **shared-addr** – Each CE is assigned a shared IPv4 address.
default-mapping-rule {**rule-ipv6-prefix** *ipv6-prefix*}	Configure the default mapping rule (DMR) to map IPv4 addresses to IPv6 addresses beyond the MAP-T domain.
description *domain-name*	Create a description for the MAP-T domain
health-check-gateway {***ipv4-addr*** | ***ipv6-addr*** | **withdraw-route**}	Configure a Health-check gateway for route withdrawn. • **withdraw-route**: • **all-link-failure** – Withdraw routes on health-check failure of all IPv4 gateways or all IPv6 gateways • **any-link-failure** – Withdraw routes on health-check failure of any gateway (default)
mtu *num*	Configure domain MTU value per domain to configure the maximum size of each packet being transmitted as determined by Transmission Control Protocol (TCP).
tcp mss-clamp {**fixed** | **none** | **subtract**}	Configure MSS to set the maximum size of a TCP segment that can be processed in a single, un-fragmented piece. • **fixed** – ACOS changes the MSS to the length you specify. A fixed MSS value must be less than or equal to the domain MTU. • **none** – ACOS does not change the MSS

Parameter	Description
	value. • **subtract** – ACOS reduces the MSS if it is longer than the specified number of bytes. This option sets the MSS based on the following calculations:

Mode Global configuration mode.

Usage This command can be used to create a new MAP-T domain on the ACOS device, or it can be used to enter the configuration level of an existing MAP-T domain in order to make changes to the domain configuration.

cgnv6 map translation fragmentation inbound

Description Configures the action to be taken when inbound IPv4 packets are too large.

Syntax

```
[no] cgnv6 map translation fragmentation inbound {drop | ipv6}
```

Parameter	Description
df-set	MAP-T behavior if Don't Fragment (DF) is set for oversize packets. By default, it is set to send-icmp.
drop	Silently drop the oversized packets. No warning or error message is sent.
ipv6	Use IPv6 fragmentation for oversized packets.

Default The default behavior is to fragment oversized packets.

Mode Global configuration mode.

Usage This command is used to configure what action should be taken when an oversized, inbound IPv4 packet is received. The default behavior is to fragment all packets.

cgnv6 map translation fragmentation inbound df-set

Description Configures the action to be taken when an inbound IPv4 packet is too large and the DF flag is set.

Syntax

```
[no] cgnv6 map translation fragmentation inbound df-set
{drop | ipv6 | send-icmp}
```

Parameter	Description
drop	Silently drop the oversized packets. No warning or error message is sent.
ipv6	Use IPv6 fragmentation for oversized packets, ignoring the DF flag.
send-icmp	Send an ICMP error message saying that the packet is too large and needs to be fragmented, but the DF flag is set.

Default The default behavior is to send an ICMP error message when oversized IPv4 packets with the DF-bit set are received.

Mode Global configuration mode.

Usage This command is used to configure what action should be taken when an oversized, inbound IPv4 packet is received and the DF flag is set.

cgnv6 map translation fragmentation outbound

Description Configures the action to be taken when an outbound IPv6 packet is too large.

Syntax

```
[no] cgnv6 map translation fragmentation outbound
{drop | ipv4 | send-icmpv6}
```

Parameter	Description
drop	Silently drop the oversized packets. No warning or error message is sent.
ipv4	Use IPv4 fragmentation for oversized packets.
send-icmpv6	Send an ICMP error message saying that the packet is too large.

Default The default behavior is to fragment oversized packets.

Mode Global configuration mode.

Usage This command is used to configure what action should be taken when an oversized, outbound IPv6 packet is received.

NPTv6

cgnv6 nptv6 domain

Description Configures NPTv6 translation to manage network traffic.

Syntax

```
[no] cgnv6 nptv6 domain name
```

This command brings you to the NPTv6 domain configuration level, where the following commands are available.

```
[no] inside-prefix ipv6addr [outside-prefix ipv6addr]
```

```
[no] outside-prefix ipv6addr
```

Parameter	Description
inside-prefix *ipv6addr*	This command specifies the inside-prefix for an NPTv6 domain.
outside-prefix *ipv6addr*	This command specifies the outside-prefix for an NPTv6 domain.

Default N/A.

Mode Configuration mode.

Usage NPTv6 translation translates the routing prefix, subnet, and interface identifier (IID) of IPv6 traffic when the traffic between networks. NPTv6 translation can be configured between an internal network and one or multiple external networks, as well as between two private networks.

cgnv6 nptv6 common send-icmpv6-on-error disable

Description Disable error notifications on NPTv6 translation failure.

Syntax `cgnv6 nptv6 common send-icmpv6-on-error disable`

Default Not set.

Mode Configuration mode.

Usage When an NPTv6 prefix translation fails, an ICMPv6 error message is sent. Use this command to disable error messages.

6rd Commands

This section describes the configuration commands for IPv6 rapid deployment (6rd). 6rd enables IPv6 clients to communicate with IPv6 servers over a service provider's IPv4 network.

cgnv6 sixrd domain

Description Configure 6rd domain settings.

Syntax

```
[no] cgnv6 sixrd domain domain-name
```

Replace *domain-name* with the string to describe the 6rd domain (1-63 characters).

This command changes the CLI to the configuration level for the specified 6rd domain, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to 6rd.

Command	Description
[no] br-ipv4-address *ipv4addr* **ipv6-prefix** *ipv6addr*/*prefix-length*	Specifies the 6rd IPv4 address of the ACOS device, and the IPv6 prefix for the 6rd domain. The IPv4 address must be one of the following: • An IP interface that is already configured on the ACOS device, on a data interface or as a floating IP address. The interface must be connected to the 6rd domain's clients. • A floating-IP interface that is already configured on the ACOS device. In this case, the High Availability (HA) state is applicable. Packets are forwarded only on the active ACOS device in the HA pair.

Command	Description
	NOTE: The current release does not support use of an anycast address for 6rd.
[**no**] **ce-ipv4-network** *ipv4addr* {*subnet-mask* | **/***mask-length*}	Specifies the client IPv4 network, and the portion of the client's 6rd customer edge (CE) router IPv4 address that is common to all of the 6rd domain's clients. For example, if your deployment uses 10.0.0.0/8 for all CE router IPv4 addresses in the 6rd domain, specify the following: **ce-ipv4-network 10.0.0.0 /8**
[**no**] **mtu** *bytes*	Specifies the maximum transmission unit (MTU) for the IPv6 tunnel. You can specify 1280-1480 bytes. The default MTU is 1480 bytes.

Default There are no 6rd domains configured by default. When you create one, it has the default settings as described in the table above.

Mode Configuration mode

Example For the ACOS BR address, you can use either an IP address configured on an ACOS interface or a High Availability (HA) floating-IP address. If you use an IP address configured on an ACOS interface, the 6rd domain is not synchronized to the standby ACOS device as part of HA configuration synchronization.

The **br-ipv4-address** command does not also configure the IPv4 interface or floating-IP address itself. The command simply indicates the configured IPv4 address that is connected to 6rd clients.

cgnv6 sixrd fragmentation inbound

Description Configure fragmentation support for oversize inbound IPv6 packets. These are packets from IPv6 servers to 6rd clients.

Syntax

```
[no] cgnv6 sixrd fragmentation  inbound
{drop | ipv4 |ipv6 | send-icmpv6}
```

Parameter	Description
drop	Drops oversize packets without sending an ICMPv6 error message back to the server. Fragmentation is not performed.
ipv4	The IPv6 packet is treated as an IPv4 payload, and the IPv4 packet is then fragmented. The client's 6rd CE router defragments the IPv4 packet, extracts the IPv6 payload, and sends it to the IPv6 client.
ipv6	The IPv6 packet is fragmented first, and the fragments are then placed into separate IPv4 packets. The IPv4 packets are not fragmented. The fragmented IPv6 packet is defragmented by the IPv6 client.
send-icmpv6	Drops oversize packets and sends an ICMPv6 error message back to the server. Fragmentation is not performed.

Default **send-icmpv6**

Mode Configuration mode

Usage For packets larger than 1500 bytes, the **ipv4** option does not work. In this case, the **ipv6** option is recommended instead.

cgnv6 sixrd fragmentation outbound

Description Configure fragmentation support for oversize outbound IPv6 packets. These are packets from the ACOS device, forwarded on behalf of 6rd clients to IPv6 servers.

Syntax

```
[no] cgnv6 sixrd fragmentation  outbound
{df-set | drop | ipv6 | send-icmp | send-icmpv6}
```

Parameter	Description
df-set	6rd behavior if Don't Fragment (DF) bit is set for oversize packets. The default is **send-icmp**.
drop	Drops oversize packets without sending an ICMPv6 error message to the client. Fragmentation is not

Parameter	Description
	performed.
ipv6	Fragments oversize IPv6 packets.
send-icmp	Drops oversize packets and sends an IPv4 ICMP error message to the client's 6rd CE router. Fragmentation is not performed.
send-icmpv6	Drops oversize packets and sends a tunneled ICMPv6 error message to the client. Fragmentation is not performed.

Default **ipv6**

Mode Configuration mode

Related Commands:

- cgnv6 sixrd fragmentation outbound df-set

cgnv6 sixrd fragmentation outbound df-set

Description Configure the ACOS response to oversize outbound IPv6 packets that have the Don't Fragment bit set.

Syntax

```
[no] cgnv6 sixrd fragmentation outbound df-set
{drop | ipv6 | send-icmp | send-icmpv6}
```

Parameter	Description
drop	Drops oversize packets without sending a tunneled ICMPv6 error message to the client.
ipv6	Fragments oversize IPv6 packets anyway and forwards the fragments.
send-icmp	Drops oversize packets and sends an IPv4 ICMP error message to the client's 6rd CE router.
send-icmpv6	Drops oversize packets and sends a tunneled ICMPv6 error message to the client.

Default **send-icmp**

Mode Configuration mode

DDoS Mitigation

acos-application-only

Description Direct BGP update messages to ACOS applications only.

Syntax

```
[no] acos-application-only
```

Mode BGP neighbour level

Usage After configuring a neighboring BGP router, route updates from this neighboring router is treated specially using the `acos-application-only` command. This configuration must be configured on the ACOS device to disable or re-enable black-listed NAT IPs.

cgnv6 ddos-protection

Description Enable or disable DDoS Mitigation for CGN.

Syntax

```
[no] cgnv6 ddos-protection {disable | enable}
```

Default Enabled.

Mode Configuration mode.

Usage DDoS protection for CGN allows for selective filtering to match traffic based on destination IP addresses and destination IP port. Selective filtering tracks the number of protocol packets received to these 2-tuples. An excess of packets is registered as a DDoS attack. ACOS then logs the IP and IP port match and drops further packets.

cgnv6 ddos-protection disable-nat-ip-by-bgp zone

Description Disable NAT IP based on BGP advertisement from upstream router.

Syntax

```
[no] cgnv6 ddos-protection disable-nat-ip-by-bgp zone name
```

Mode Configuration mode.

Usage When an IP is black-listed, upon receiving a BGP route update, ACOS device can disable a specific NAT IP fallen into the configured BGP DDoS zone.

cgnv6 ddos-protection logging

Description Enable or disable logging statistics for DDoS Mitigation.

Syntax

```
[no] cgnv6 ddos-protection logging {disable | enable}
```

Default Enabled.

Mode Configuration mode.

Usage When selective filtering identifies 2-tuples that are being flooded and drop the packets, ACOS can log the number of packets over the threshold that are dropped.

cgnv6 ddos-protection max-hw-entries

Description Configure a limit for Selective Filtering entries in the hardware. The command is applicable only to FTA-devices.

Syntax

```
[no] cgnv6 ddos-protection max-hw-entries number
```

Mode Configuration mode.

Usage On platforms that support Selective Filtering at the hardware level, a lower limit for Selective Filtering entries can be configured in the hardware.

cgnv6 ddos-protection packets-per-second

Description Configure the maximum number of packets allowed per protocol for either an entire IP or any given combination of a destination IP and IP port.

Syntax

```
[no] cgnv6 ddos-protection packets-per-second
{include-existing-session | ip | other | tcp | udp}
num  action {log | drop} expiration seconds
```

Parameter	Description
include-existing-session	Count traffic associated with an existing session into the packets-per-second. The default is disabled.
ip | other | tcp |	Traffic type.

Parameter	Description
udp	• **ip** - Configure packets-per-second threshold per IP. The default is 3000000. • **other** - Configure packets-per-second threshold for other L4 protocols. The default is 10000. • **tcp** - Configure packets-per-second threshold per TCP port. The default is 3000.x • **udp** - Configure packets-per-second threshold per UDP port. The default is 3000.
num	Maximum number of packets per second allowed. The maximum configurable limit is 30000000 packets.
action {log | drop} **expiration** *seconds*	Specify the action to be taken when the packets are received. The following actions are available: • **log** - Log the event without dropping the packets. • **drop** - Log, and drop all packets (default). **expiration** - Specify the time (in seconds), after which the L4 entries expire. The default value is based on the traffic type: • TCP/UDP/Other: The default value is 30 seconds. • IP: The default value is 3600 seconds.

Default Selective filtering is enabled by default. The default value is 3000 packets for TCP or UDP protocol, exclusive, or 3000 packets per source-IP. For all other protocols combined, the default value is 10000 packets.

Mode Configuration mode.

Usage DDoS protection for CGN allows for selective filtering to match traffic based on destination IP addresses and destination IP port. Selective filtering tracks the number of protocol packets received to these 2-tuples. An excess of packets is registered as a DDoS attack, and all packets above the configured threshold are dropped.

Filtering is performed in two stages:

- Stage 1: If the IP entry is created, a L4 entry will not be created since all ports of this IP are dropped. Conversely, if the L4 entry is created, an IP entry will also be created if the packets-per-second to a single NAT IP exceeds the configured DDoS protection packets-per-second IP threshold. In this scenario, the processing moves to Stage 2.
- Stage 2: Processing depends on the Layer 4 protocol:
  - TCP/UDP – If the "bad" packets-per-second to a single (NAT IP:port) pair exceeds the configured threshold, then that pair gets the selective filtering entry. For example, if UDP packets that hit a NAT IP on port 5000 exceed the threshold, then only UDP packets to port 5000 will be blocked. Other UDP packets to that NAT IP will not be affected.
  - Other Layer 4 protocols – If the "bad" packets-per-second to a single (NAT IP: Layer 4 protocol) pair exceeds the configured threshold, that pair gets an entry. For example, if GRE (ip protocol 47) packets to one NAT IP exceeds the threshold for Other protocols, then only GRE packets to that NAT IP will be blocked.

cgnv6 ddos-protection packets-per-second ip

Description Configure the action to be taken when the packets-per-second (PPS) threshold (default 3000000) per IP exceeds.

Syntax

```
[no] cgnv6 ddos-protection packets-per-second ip  threshold
action {log | drop | redistribute-route route-map-name
expiration seconds remove-wait-timer seconds timer-multiply-
max num forward }
```

Parameter	Description
action {log | drop | redistribute-route *route-map-name*} **expiration** *seconds* **remove-wait-timer** *seconds* **timer-multiply-max** *num* **forward**	When the ACOS device detects a DDoS attack i.e., when the DDoS protection threshold is breached, one of the following actions can be configured: • **log** - Log the event only. • **drop** - Log the event, drop all packets, and mark the NAT IP as unusable. This is the default action. • **redistribute-route** - Log the event, redirect the packets to an upstream router via Border Gateway Protocol (BGP), and stop rate-limiting. The *route-map-name* parameter specifies the route-map to be used for redirecting the packets. Configuring this option enables the Remotely Triggered Black Hole (RTBH) protection technique. Additional parameters available while configuring RTBH: • **expiration** If the action configured is **drop**, this parameter specifies the duration (in seconds) the NAT IP traffic must be below the configured packets-per-second threshold before it is removed from the blacklist. If the action configured is **redistribute-route**, this parameter specifies the duration (in minutes) the blocked route must be disabled when a DDoS attack is detected. ACOS removes the blackhole route remotely

Parameter	Description
	when this duration expires. You can specify a value in the range of 10 to 8640000. The default value is 3600 seconds. This parameter is also available for **log** and **drop** actions. • **remove-wait-timer** – Specifies the maximum time (in seconds) to wait before removing an NAT IP from the black list. You can specify a value in the range of 0 to 300. The default value is 300. • **timer-multiply-max** - Specify the maximum value of the timer multiplier for attacks that last long. You can specify a value in the range of 1 to 100. The default value is 6. During the remove-wait period, if ACOS detects a DDoS attack again, the black hole entry is re-initiated and the blackhole timer is extended by a duration that is twice the expiration time (for the first time). The second time, the duration is thrice the expiration time, and this duration continues to increment until it reaches the maximum limit specified by this parameter. • **forward** - Specify this option to forward the traffic (instead of dropping it unconditionally) and continue rate-limiting. This will allow subscribers to access the NAT IP under attack even when RTBH is in effect.
threshold	The maximum number of packets per second allowed before an IP is blacklisted. The

Parameter	Description
	maximum configurable limit is 30000000 packets.

Default Disabled

Mode Configuration Mode

Usage DDoS protection is triggered only when the configured *threshold* is breached.

Example The following example demonstrates the usage of **log** action. In this example, when the PPS limit exceeds 10000, an event is logged.

```
ACOS(config)# cgnv6 ddos-protection packets-per-second ip
10000 action log
```

Example The following example demonstrates the usage of **drop** action. When the PPS limit exceeds 25000, an event is logged and ACOS drops all incoming packets. The NAT IP is marked as unusable, and the existing sessions are cleared.

```
ACOS(config)# cgnv6 ddos-protection packets-per-second ip
25000 action drop
```

Example The following example demonstrates the usage of **redistribute-route** action. In this example, when the PPS limit exceeds 10000, the RTBH action is triggered.

```
ACOS(config)# cgnv6 ddos-protection packets-per-second ip
10000 action redistribute-route mymap
```

Example The following example demonstrates the usage of the **forward** option. When the PPS limit exceeds 10000, the RTBH action is triggered. However, since the **forward** option is set, the packets are forwarded (instead of being dropped).

```
ACOS(config)# cgnv6 ddos-protection packets-per-second ip
10000 action redistribute-route mymap forward
```

For more information, refer to the *IPv4-to-IPv6 Transition Solutions Guide*.

cgnv6 ddos-protection syn-cookie

Description Configure SYN cookie protection in CGNAT deployment.

Syntax

```
[no] cgnv6 ddos-protection syn-cookie enable} tcp-half-open
on-threshold <number> on-timeout <number>
```

Parameter	Description
on-threshold *<num>*	The threshold for TCP half-open sessions. SYN cookie protection is enabled after the specified threshold exceeds.
on-timeout *<num>*	The SYN cookie timeout. SYN cookie protection is disabled after the specified timeout expires. The default timeout value is 120 seconds.

Default Disabled

Mode Configuration mode.

Usage This command configures TCP SYN cookie protection for CGN. It is triggered after the number of tcp-half-open sessions exceeds the configured threshold and is disabled after the timeout value expires.

In a CGN + firewall deployment, if you configure syn-cookie protection for a firewall rule, the configuration in the firewall rule overrides the configuration in this command.

Example The following example configures syn-cookie protection for CGN:

```
ACOS(config)#cgnv6 ddos-protection syn-cookie enable
```

Example The following example configures SYN cookie in the CGN and disables it in a firewall rule-set. For the CGN traffic matching the rule, the SYN cookie protection will be disabled:

```
ACOS(config)#cgnv6 ddos-protection syn-cookie enable
ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn lid)# source-nat-pool lsnpool1
!
rACOS(config)#rule-set rs1
ACOS(config-rule set:rs1)#rule 3
ACOS(config-rule set:rs1-rule:3)#action-group
```

```
ACOS(config-rule set:rs1-rule:3-action-group)#permit cgnv6
lsn-lid 1
ACOS(config-rule set:rs1-rule:3-action-group)#permit tcp syn-
cookie disable
```

cgnv6 lsn-lid conn-rate-limit

Description Within an LSN LID, you can enable connection rate limiting. This configures a maximum number of connections a client can attempt to initiate per second.

Syntax

```
[no] cgnv6 lsn-lid num
```

Replace *num* with the LSN LID number, 1-1023.

This command changes the CLI to the configuration level for the specified LSN LID, where the following commands are available.

NOTE: The other configuration commands at this level are not applicable to LSN DDoS Mitigation.

Command	Description
[no] conn-rate-limit *num*	The maximum number of connections a client can attempt to initiate per second. The value can range from 1-65535.

Default The LSN LID has the following default value:

- **conn-rate-limit** – No limit

Mode CGNv6 LSN LID mode

Example The following commands enable connection rate limiting on an LSN LID with the ID number 10. The connection rate is limited to 100 connections per second. The LID can then be bound to any CGNv6 class-list.

```
ACOS(config)# cgnv6 lsn-lid 10
ACOS(config-lsn-lid)# conn-rate-limit 100
```

NOTE: The default is to have no connection rate limit except for the maximum number of connections allowed, if configured elsewhere. Any value from 1 to 65535 connections per second are allowed.

ip anomaly-drop

Description Enable filtering for IP packets that exhibit predictable, well-defined anomalies. You can enable filtering for specific IP anomalies, or you can enable filtering for the following types of IP anomalies:

Syntax

```
[no] ip anomaly-drop
[drop-all | frag | ip-option | ipv6-ext-header | land-attack |
packet-deformity { layer-3 | layer-4 } | ping-of-death |
security-attack { layer-3 | layer-4 } | tcp-no-flag | tcp-syn-
fin | tcp-syn-frag ]
```

Command	Description
drop-all	Drop all packets with IP anomalies.
frag	Drop all fragmented packets.
ip-option	Drop packets that have IP options
ipv6-ext-header	See ip anomaly-drop ipv6-ext-header.
land-attack	Drop packets that have the same source and destination address.
packet-deformity {layer-3 | layer-4}	Drop packets with deformities. • `layer-3` - network layer anomaly. • `layer-4` - transport layer anomaly.
security-attack {layer-3 | layer-4}	Drop packets causing security attack. • `layer-3` - network layer anomaly. • `layer-4` - transport layer anomaly.
ping-of-death	Drop oversized ICMP packets.
tcp-no-flag	Drop TCP packets that have no flag.
tcp-syn-fin	Drop TCP packets that have both SYN and FIN flags set.
tcp-syn-frag	Drop fragmented TCP packets that have SYN flag set.

Default All options are disabled by default.

Example The following commands enable filtering and dropping of each group of IP anomalies:

```
ACOS(config)# ip anomaly-drop packet-deformity layer-3
ACOS(config)# ip anomaly-drop packet-deformity layer-4
ACOS(config)# ip anomaly-drop security-attack layer-3
ACOS(config)# ip anomaly-drop security-attack layer-4
```

ip anomaly-drop ipv6-ext-header

Description Enable filtering of IP packets based on the IPv6 Extension Headers (EHs).

Syntax

```
[no] ip anomaly-drop ipv6-ext-header
 [ auth | { hop-by-hop | dest | routing [ option-type num1 [
to num2 ] ] } | eh-type num1 [ to num2 ] | esp | frag |
malformed | mobility | no-next ]
```

Command	Description
auth	Specify this option to drop all packets that contain the Authentication EH.
hop-by-hop [option-type *num1* **[to** *num2* **]]**	Specify this option to drop all packets that contain the Hop-By-Hop EH (irrespective of the Option Type) or drop the packets that contain a specific Option Type in the Hop-By-Hop EH. You can specify a particular value (*num1*) for the Option Type in the EH or you can specify a range (*num1* to *num2*) for the Option Types. You can enter values in the range 0 to 255. For example, if you specify a range from 100 to 200, all packets with Hop-By-Hop EH having the Option Types in the range 100 to 200 will be dropped. **NOTE**: Option Type 1 is often used for padding. Therefore, this field is set implicitly in most IPv6 packets. If you configure the **option-type** as 1, most of the IPv6 packets, including the non-malicious packets, will be dropped.

Command	Description
dest [option-type *num1* **[to** *num2* **]]**	Specify this option to drop all packets that contain the Destination EH (irrespective of the Option Type) or drop the packets that contain a specific Option Type in the Destination EH. You can specify a particular value (*num1*) for the Option Type in the EH or you can specify a range (*num1* to *num2*) for the Option Types. You can enter values in the range 0 to 255. For example, if you specify a range from 100 to 200, all packets with Destination EH having the Option Types in the range 100 to 200 will be dropped. **NOTE**: Option Type 1 is often used for padding. Therefore, this field is set implicitly in most IPv6 packets. If you configure the option-type as 1, most of the IPv6 packets, including the non-malicious packets, will be dropped.
routing [option-type *num1* **[to** *num2* **]]**	Specify this option to drop all packets that contain the Routing EH (irrespective of the Routing Type) or drop the packets that contain a specific Routing Type in the Routing EH. You can specify a particular value (*num1*) for the Routing Type in the EH or you can specify a range (*num1* to *num2*) for the Routing Types. You can enter values in the range 0 to 255. For example, if you specify a range from 160 to 201, all packets with Routing EH having the Routing Types in the range 160 to 201 will be dropped.
eh-type *num1* **[to** *num2*]	Specify this option to drop all packets that contain an unknown Extension Header type. You can specify a particular value (*num1*) or specify a range (*num1*) to (*num2*) for the unknown extension

Command	Description
	header types. You can enter values in the range 0 to 255. For example, if you specify a range from 150 to 180, all packets with the Extension Header types in the range 150 to 180 will be dropped. **NOTE:** You must specify values other than 0, 43, 44, 50, 51, 59, 60, and 135. These IDs are set for the eight well-known IPv6 extension headers.
esp	Specify this option to drop all packets that contain the Encapsulation Security Payload (ESP) EH.
frag	Specify this option to drop all packets that contain the Fragmentation EH.
malformed	Specify this option to drop packets with malformed EHs. When this option is configured, the order of the extension headers (as per the RFC2460 standard) and the number of occurrences of the extension headers are checked. An IPv6 packet is considered as malformed if the extension header order is not followed or the number of occurrences of the extension header is different than expected. This option can be configured to detect and drop such malformed IPv6 packets.
mobility	Specify this option to drop all packets that contain the Mobility EH.
no-next	Specify this option to drop all packets that contain the No-Next EH.

Default All options are disabled by default.

Usage This command can be enabled globally at the system level; it cannot be enabled at the partition level.

NOTE:

- Hardware FTA does not accelerate the detection and filtering of IPv6 Extension Header based anomalies.
- The filtering of IPv6 Extension Header based anomalies is not logged.

Example The following example enables the filtering of packets that contain the Authentication EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header auth
```

Example The following example enables the filtering of packets that contain the ESP EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header esp
```

Example The following example enables the filtering of packets with malformed EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header malformed
```

Example The following example enables the filtering of packets that contain the Hop-By-Hop EH with Option Type in the range 194 to 201:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header hop-by-hop
option-type 194 to 201
```

Example The following example enables the filtering of packets that contain Destination EH with Option Type 110:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header dest option-type
110
```

Example The following example enables the filtering of packets that contain unknown EH having protocol ID 100:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header eh-type 100
```

Example The following example enables the filtering of packets that contain Routing EH with Routing Type 160:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header dest option-type
160
```

Show Commands

clear cgnv6 ddos-protection disabled-ip-by-bgp

Description Clear the currently disabled NAT IP on BGP advertisement.

Syntax

```
clear cgnv6 ddos-protection disabled-ip-by-bgp {all | ip-address ip-addr}
```

Mode Configuration mode

clear cgnv6 ddos-protection ip-entries

Description Clear DDoS IP entries.

Syntax

```
clear cgnv6 ddos-protection ip-entries {all | ip-address ip-addr | nat-pool name}
```

Mode Configuration mode

clear cgnv6 ddos-protection l4-entries

Description Clear DDoS L4 entries.

Syntax

```
clear cgnv6 ddos-protection l4-entries {address ipaddr | all | l4-proto protocol-num | nat-pool name | port port-num}
```

Mode Configuration mode

clear cgnv6 ddos-protection statistics

Description Clear DDoS statistics.

Syntax

```
clear cgnv6 ddos-protection statistics
```

Mode Configuration mode

show cgnv6 ddos-protection disabled-ip-by-bgp

Description This command displays the list of NAT IPs disabled on BGP advertisement.

Syntax

```
show cgnv6 ddos-protection disabled-ip-by-bgp
```

Example The following example displays sample output for the **show cgnv6 ddos-protection disabled-ip-by-bgp** command:

```
ACOS# show ddos-protection disabled-ip-by-bgp
IP Address            NAT Pool Name
===================================
1.1.1.1                 2
1.1.1.2                 2
```

show cgnv6 ddos-protection ip-entries

Description This command displays abnormal IP entries from DDoS monitoring and selective filtering.ip-en

Syntax

```
show cgnv6 ddos-protection ip-entries [all]
```

Mode All

Example The following example displays sample output for the **show cgnv6 ddos-protection ip-entries** command:

```
ACOS(config)#show cgnv6 ddos-protection ip-entries
Address               PPS          Expiration
-------------------------------------------
15.15.15.15           5000           3600
```

The following example displays sample output for the show cgnv6 ddos-protection ip-entries all command:

```
ACOS(config)# show cgnv6 ddos-protection ip-entries all
(*) L4 PPS Threshold Exceeded
(**) L3 PPS Threshold Exceeded

Address               PPS          Expiration   L4-Entries
-----------------------------------------------------------
```

```
15.15.15.15          0            -            0
```

NOTE: If you enter the `all` parameter, it lists all the NAT IPs and marks an entry if it is a L4 entry or IP entry.

show cgnv6 ddos-protection l4-entries

Description This command displays abnormal L4 port entries from DDoS monitoring and selective filtering.

Syntax

```
show cgnv6 ddos-protection l4-entries
[address ipaddr | in-hardware | l4-proto protocol-num |
not-in-hardware | port port-num]
```

Example The following example displays sample output:

```
ACOS(config)# show cgnv6 ddos-protection l4-entries
Address          L4    Port    PPS Expiration
-----------------------------------
1.1.1.1          UDP   333     5000 86
```

Usage The following table describes the fields for the show command output:

Field	Description
Address	The destination IP address that traffic is matched to.
L4	The Layer 4 protocol type. In the above example, L4 17 indicates UDP traffic.
Port	The specific destination IP port that traffic is matched to.
PPS	The number of packets that match the IP address and the given port in the last 10 seconds.
Expiration	The number of seconds after which the L4 entries expire. **NOTE:** The expiration value is updated every 10 seconds in case of L4 entries and every second in case of IP entries.

show cgnv6 ddos-protection statistics

Description This command displays the logging statistics for CGN DDoS selective filtering.

Syntax

```
show cgnv6 ddos-protection statistics
```

Mode All

Example The following is a sample output:

```
AX5100(config)#show cgnv6 ddos-protection statistics
L3 Entry Added                              0
L3 Entry Deleted                            0
L3 Entry Added to BGP                       0
L3 Entry Removed From BGP                   0
L3 Entry Added to HW                        0
L3 Entry Removed From HW                    0
Too Many L3 entries                         0
L3 Entry Match Drop                         0
HW L3 Entry Match Drop                      0
L3 Entry Drop due to HW Limit Exceeded      0
L4 Entry Added                              0
L4 Entry Deleted                            0
L4 Entry Added to HW                        0
L4 Entry Removed From HW                    0
HW out of L4 Entries                        0
L4 Entry Match Drop                         0
HW L4 Entry Match Drop                      0
L4 Entry Drop due to HW Limit Exceeded      0
TCP SYN cookie SYN ACK Sent                 0
TCP SYN cookie verification passed          0
TCP SYN cookie verification failed          0
```

show cgnv6 dns64 statistics

Description Show statistics for DNS64.

Syntax

```
show cgnv6 dns64 statistics
```

Mode Privileged EXEC and all configuration levels

Usage

The following command shows DNS64 statistics:

```
ACOS# show cgnv6 dns64 statistics
DNS Service Type: dns64
Query      Q-Parallel Q-Passive  Q-Changed  Q-Bad
Response Translated Cache Dropped  R-Bad R-Error R-Empty
-----------------------------------------------------
0          0          0     0       0
0          0          0     0       0      0       0
```

The following table describes the fields in the command's output.

Field	Description
Query	Number of queries received from clients.
Response	Number of responses received from the DNS server. **NOTE:** The ACOS can send multiple queries to the server for a single query from a client. In this case, the Query counter will increment by only 1 for the client's request, while the Response counter will increment by 1 for each response to each individual query sent by the ACOS device to the DNS server. For example, a single client query can result in an increment of 1 for Query and an increment of 2 for Response.
Q-Parallel	Number of parallel queries sent out by the ACOS device.
Translated	Number of A responses translated by DNS64 into AAAA responses.
Q-Passive	Number of times DNS64 sent an A query to the DNS server, because the server sent an empty response or error in response to a AAAA query.
Cache	Number of times a AAAA reply was sent from the DNS64 cache.
Q-Changed	When the change-query option is enabled in the DNS template, this counter indicates the number of AAAA queries converted into A queries by DNS64.

Field	Description
Dropped	When the passive-query option is disabled in the DNS template, this counter indicates the number of empty responses or errors received from the DNS server.
Q-Bad	Number of bad (malformed) query packets received on the DNS virtual port.
R-Bad	Number of bad (malformed) response packets sent to the DNS server.
R-Error	Number of DNS server responses with errors.
R-Empty	Number of empty responses from the DNS server.

show cgnv6 ds-lite alg

Description Show the current Application Level Gateway (ALG) configuration for DS-Lite.

Syntax

```
show cgnv6 ds-lite alg {ftp | h323 | mgcp | pptp | rtsp | sip | tftp} config
```

Mode All

show cgnv6 ds-lite full-cone-sessions

Description Shows currently active full-cone sessions.

Syntax

```
show cgnv6 ds-lite full-cone-sessions [pcp | pool pool-name]
```

The *pool-name* option displays sessions only for the specified pool. If you omit this option, sessions for all pools are shown.

The **pcp** options only displays full-cone sessions created by PCP requests.

Mode All

The following table describes the fields in this command's output.

Field	Description
Information for Individual Sessions:	
Protocol	Layer 4 protocol of the session.
Inside IPv6	Client DS-Lite router's IPv6 address.
Inside Address	Client's IPv4 address.
NAT Address	Global IPv4 address assigned to the client by the ACOS device for communicating with the IPv4 server.
Inbound	Number of inbound connections.
Outbound	Number of outbound connections.
Pool	IP address pool from which the NAT address was assigned.
CPU	ACOS CPU on which the session resides.
Age	Number of seconds the session has been in effect.
Flags	Value used by A10 Technical Support.
Statistics (brief option)	
DS-Lite TCP Full-cone Session Created	Number of TCP full-cone sessions created.
DS-Lite TCP Full-cone Session Freed	Number of TCP full-cone sessions freed.
DS-Lite UDP Full-cone Session Created	Number of UDP full-cone sessions created.
DS-Lite UDP Full-cone Session Freed	Number of UDP full-cone sessions freed.
DS-Lite Full-cone Session Creation Failed	Number of times an attempt to create a DS-Lite full-cone session failed.

show cgnv6 ds-lite inside-user

Description Show session information for a specific DS-Lite inside client.

Syntax

```
show cgnv6 ds-lite inside-user ipv6addr
```

Replace *ipv6addr* with the inside IPv6 address of the user.

Mode All

Example The following command shows session information for DS-Lite user 2001:10::100:

```
ACOS# show cgnv6 ds-lite inside-user 2001:10::100
DS-Lite User-Quota Sessions:
Inside IPv6       NAT Address   ICMP   UDP    TCP    Pool    LID   Flag
------------------------------------------------------------------------
--
2001:10::100       172.7.7.30     0      2      2      lsn0    1     U
Total User-Quota Sessions Shown: 1

DS-Lite Full Cone Sessions:
Prot Inside IPv6                                    Inside Address
     NAT Address            Conns  Pool             CPU Age
------------------------------------------------------------------------
------------------------------------------------------------------
TCP  2001:10::100
10.10.10.100:26504     172.7.7.30:27656       0      lsn0             2
  120
UDP  2001:10::100
10.10.10.100:48968     172.7.7.30:52232       1      lsn0             4
  -
UDP  2001:10::100
10.10.10.100:51775     172.7.7.30:29759       1      lsn0             4
  -
TCP  2001:10::100
10.10.10.100:26505     172.7.7.30:35849       1      lsn0             1
  -
Total Full Cone Sessions: 4

DS-Lite Data Sessions:
```

```
Prot IP Type  IP Address and Port
       Age  Hash Flags
------------------------------------------------------------------------
-----------------------
Tcp  Fwd Src  [2001:10::100]10.10.10.100:26505
       0    1    NS
     Fwd Dst  [2001:10::1]172.7.7.100:80
     Rev Src  172.7.7.100:80
     Rev Dst  172.7.7.30:35849
Udp  Fwd Src  [2001:10::100]10.10.10.100:51775
       300  4    NS
     Fwd Dst  [2001:10::1]172.7.7.100:5300
     Rev Src  172.7.7.100:5300
     Rev Dst  172.7.7.30:29759
Udp  Fwd Src  [2001:10::100]10.10.10.100:48968
       300  4    NS
     Fwd Dst  [2001:10::1]172.7.7.100:5300
     Rev Src  172.7.7.100:5300
      Rev Dst  172.7.7.30:52232
```

The following table describes the fields in the command's output.

Field	Description
DS-Lite User-Quota Sessions	Lists the following user-quota session information for the user: • Inside IPv6 – IPv6 address of the remote end of the tunnel • NAT Address – Client IPv4 NAT address from the LSN pool on the ACOS device • ICMP – Number of ICMP sessions from the quota that are in use • UDP – Number of UDP sessions from the quota that are in use • TCP – Number of TCP sessions from the quota that are in use • Pool – LSN NAT pool from which the NAT

Field	Description
	address for the session was selected • LID – Limit ID (LID) in which the user quota is configured
DS-Lite Full-Cone Sessions	Lists the following information for the user's full-cone session: • Prot – Protocol of the session • Inside IPv6 – IPv6 address of the remote end of the tunnel • Inside Address – IPv4 address and protocol port of the client • NAT Address – Client IPv4 NAT address from the LSN pool on the ACOS device • Conns – Number of connections currently using the session • Pool – LSN NAT pool from which the NAT address for the session was selected • CPU – ACOS CPU on which the session resides • Age – Number of seconds the session has been in effect
DS-Lite Data Sessions	Lists the following data session information for the user: • Prot – Protocol of the session • IP Type – Role of the IP address in the session: ◦ Fwd Src – IPv6 address of the remote end of the tunnel, and IPv4 address and protocol port of the client ◦ Fwd Dst – IPv6 address of the tunnel interface on the ACOS device,

Field	Description
	and IPv4 address and protocol port of the server ◦ Rev Src – IPv4 address and protocol port of the server ◦ Rev Dst – Client IPv4 NAT address from the LSN pool on the ACOS device • IP Address and Port – IP addresses and protocol ports of the session • Age – Number of seconds the session has been in effect • Hash – Hash value for the session • Flags – This value is used by A10 Technical Support.

show cgnv6 ds-lite nat-address

Description Show DS-Lite sessions filtered by NAT address.

Syntax

```
show cgnv6 ds-lite nat-address nataddr [nat-port natport]
```

Parameter	Description
nataddr	Specifies the NAT IP address.
natport	Specifies the NAT port.

Mode All

Example The following command shows DS-Lite session information filtered by NAT address for user 9.9.9.73.

```
ACOS# show cgnv6 ds-lite nat-address 9.9.9.73
Prot IP Type  IP Address and Port
                Age  Hash Flags    Type
-----------------------------------------------------------------
-----------------------------------
```

```
Udp  Fwd Src  [3201::172]121.78.233.82:2468
               300  4    NSe0f0r0 LSN
     Fwd Dst  [3201::200]9.9.9.173:10000
     Rev Src  9.9.9.173:10000
     Rev Dst  9.9.9.73:62178
Udp  Fwd Src  [3201::172]166.179.148.63:2469
               300  5    NSe0f0r0 LSN
     Fwd Dst  [3201::200]9.9.9.173:10000
     Rev Src  9.9.9.173:10000
     Rev Dst  9.9.9.73:62183
Total Sessions:          2
```

Example The following command shows DS-Lite session information filtered by NAT address for user 9.9.9.73 and NAT port 62183.

```
ACOS# show cgnv6 ds-lite nat-address 9.9.9.73 nat-port 62183
Prot IP Type  IP Address and Port
               Age  Hash Flags    Type
-------------------------------------------------------------
-----------------------------------
Udp  Fwd Src  [3201::172]166.179.148.63:2469
               180  5    NSe0f0r0 LSN
     Fwd Dst  [3201::200]9.9.9.173:10000
     Rev Src  9.9.9.173:10000
     Rev Dst  9.9.9.73:62183
Total Sessions:          1
```

The following table describes the fields in this command's output

Field	Description
Prot	Layer 4 protocol of the session.
IP Type	The type of IP address: • Fwd Src - Forward Source • Fwd Dst - Forward Dest • Rev Src - Reverse Source • Rev Dst - Reverse Dest
IP Address and	IP address and port number for the

Field	Description
Port	corresponding IP Type
Age	Number of seconds since the session started.
Hash	CPU ID.
Flags	Processing path for the traffic: • NF – Fast-path processing. • NS – Slow-path processing.
Type	Type of NAT traffic.

show cgnv6 ds-lite port-reservations

Description Show Layer 4 port reservations.

Syntax

```
show cgnv6 ds-lite port-reservations
```

Mode All

The following table describes the fields in this command's output.

Field	Description
Tunnel Src IPv6 Address	Source IPv6 address of the tunnel on which the ACOS device receives the client traffic.
Tunnel Dst IPv6 Address	Destination IPv6 address of the tunnel on which the ACOS device receives the client traffic.
Inside Address	Client IPv4 address.
Inside Start Port	Beginning Layer 4 protocol port number in the port range to be mapped.
Inside End Port	Ending Layer 4 protocol port number in the port range to to be mapped.
NAT Address	Public IPv4 address to map to the client IPv4 address.
NAT Start Port	Beginning Layer 4 protocol port number to map to the inside port range.

Field	Description
NAT End Port	Ending Layer 4 protocol port number to map to the inside port range.

show cgnv6 ds-lite statistics

Description Show global statistics related to DS-Lite.

Syntax

```
show cgnv6 ds-lite statistics
```

Mode All

The following table describes the fields in this command's output.

Field	Description
Total TCP Ports Allocated	Total number of TCP ports allocated for user sessions.
Total TCP Ports Freed	Total number of TCP ports freed for use by other sessions.
Total UDP Ports Allocated	Total number of UDP ports allocated for user sessions.
Total UDP Ports Freed	Total number of UDP ports freed for use by other sessions.
Total ICMP Ports Allocated	Total number of ICMP ports allocated for user sessions.
Total ICMP Ports Freed	Total number of ICMP ports freed for use by other sessions.
Data Session Created	Total number of data sessions created.
Data Session Freed	Total number of data sessions freed.
User-Quota	Number of port mappings created for which the

Field	Description
Created	user quota had available mappings.
User-Quota Freed	Number of port mappings that were created for which the user quota had available mappings, that were later freed.
User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
TCP NAT Port Unavailable	Number of times a TCP port for an LSN NAT session was unavailable.
UDP NAT Port Unavailable	Number of times a UDP port for an LSN NAT session was unavailable.
ICMP NAT Port Unavailable	Number of times an ICMP port for an LSN NAT session was unavailable.
New User NAT Resource Unavailable	Number of times LSN resources (ICMP, TCP, or UDP) were not available for a new user.
TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
Extended User-Quota Matched	Number of times the extended user quota was used to create a mapping.
Extended User-Quota Exceeded	Number of times a NAT port was unavailable to a client because the client had exceeded the extended user quota.

Field	Description
Data Session User-Quota Exceeded	Number of times a client exceeded their data session quota.
TCP Full-cone Session Created	Total number of LSN TCP full-cone sessions created.
TCP Full-cone Session Freed	Total number of LSN TCP full-cone sessions freed.
UDP Full-cone Session Created	Total number of LSN UDP full-cone sessions created.
UDP Full-cone Session Freed	Total number of LSN UDP full-cone sessions freed.
Full-cone Session Creation Failed	Number of times creation of a full-cone session failed.
Hairpin Session Created	Total number of LSN hairpin sessions created.
Self-Hairpinning Drop	Number of hairpin sessions dropped because the source and destination client were the same.
Endpoint-Independent Mapping Matched	Number of times LSN reused the LSN mapping assigned to a client for subsequent traffic for that client. (This is the benefit provided by Endpoint independent mapping.)
Endpoint-Independent Filtering Matched	Number of times traffic from any source to a given mapped client was forwarded to the internal client, regardless of the endpoint. (This is the benefit provided by Endpoint independent filtering.)
Endpoint-	Number of times traffic to a mapped client was

Field	Description
Dependent Filtering Drop	dropped because endpoint-independent filtering was not enabled, and the traffic was not from the endpoint mapped to the client.
Endpoint-Independent Filtering Inbound Limit Exceeded	Number of times the maximum number of Endpoint-Independent Filtering (EIF) sessions allowed for a NAT mapping was exceeded.
NAT Pool Mismatch Drop	Number of times traffic was dropped because matching traffic for a current full-cone session or user-quota session uses a different pool or pool group than the one redirected to by the rule list.
TCP Port Overloaded	Number of times a TCP port on a NAT address was assigned to a new client while another client was still using the mapping. **NOTE:** This counter and the other Port Overloading counters apply only if port overloading is configured.
UDP Port Overloaded	Number of times a UDP port on a NAT address was assigned to a new client while another client was still using the mapping.
TCP Port Overloading Session Created	Number of times a session on an overloaded TCP port was created.
UDP Port Overloading Session Created	Number of times a session on an overloaded UDP port was created.
TCP Port Overloading Session Freed	Number of times a session created on an overloaded TCP port was freed.

Field	Description
UDP Port Overloading Session Freed	Number of times a session created on an overloaded UDP port was freed.
NAT Pool Unusable	Number of times traffic hit a disabled NAT IP.
HA NAT Pool Unusable	Number of times traffic hit a disabled NAT IP in high availability standby state.
HA NAT Pool Batch Type Mismatch	
No RADIUS Profile Match	Number of times traffic did not match the RADIUS profile.
Truncated Packet	Number of tunneled packets that were truncated because they were longer than the Maximum Transmission Unit (MTU) on the ACOS interface where the packet was received.
LSN LID Drop	Number of times traffic matched the drop action in the LSN LID, and was dropped.
LSN LID Pass-through	Number of times traffic matched the pass-through action in the LSN LID, and was passed through without being NATted.
No Class-List Match	Number of times traffic did not match the LSN class list.
Permit Class-List Drop	Number of packets dropped because they did not match the class list's permit list.

show cgnv6 ds-lite user-quota-sessions

Description Shows currently active user quota sessions.

Syntax

```
show cgnv6 ds-lite user-quota-sessions
[pool pool-name]
[top num  {all | icmp | tcp | udp}]
```

Parameter	Description
pool *pool-name*	Shows currently active full-cone sessions only for the specified pool. If you omit this option, sessions for all pools are shown.
top *num* *type*	Limits the display to the sessions with the highest counters for the specified resource type. You can specify 1-100. The resource type can be one of the following: • **all** – Displays the sessions with the highest counters for all resource types (ICMP, TCP, and UDP). • **icmp** – Displays the sessions with the highest counters for ICMP. • **tcp** – Displays the sessions with the highest counters for TCP. • **udp** – Displays the sessions with the highest counters for UDP.

Mode All

Example The following command shows ds-lite user-quota information:

```
ACOS# show cgnv6 ds-lite user-quota-sessions
DS-Lite User-Quota Sessions:
Inside IPv6 Prefix  NAT Address  ICMP   UDP    TCP    Session
UDP Session TCP Session Pool      LID   Flag
------------------------------------------------------------------
--------------------
2001:20:20:20::75       128     10.2.0.96    0     12893  8668
 21561    12893        8668         p1    1     -
Total User-Quota Sessions: 1
```

The following table describes the fields in this command's output.

Field	Description
DS-Lite User-Quota Created	Number of port mappings created for which the user quota had available mappings.
DS-Lite User-Quota Freed	Number of port mappings that were created for which the user quota had available mappings, that were later freed.
DS-Lite User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
DS-Lite TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
DS-Lite UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
DS-Lite ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
DS-Lite Extended User-Quota Matched	Number of times the extended user quota was used to create a mapping.
DS-Lite Extended User-Quota Exceeded	Number of times a NAT port was unavailable to a client because the client had exceeded the extended user quota.
DS-Lite Data Session User-Quota Exceeded	Number of times a client exceeded their data session quota.
Information for Individual Sessions:	
Inside IPv6	Client DS-Lite router's IPv6 address.
NAT	Public IP address assigned to the client by DS-Lite.
ICMP	Number of ICMP sessions from the quota that are in use.
UDP	Number of UDP sessions from the quota that

Field	Description
	are in use.
TCP	Number of TCP sessions from the quota that are in use.
Session UDP	Number of UDP sessions from the quota that are in use.
Session TCP	Number of TCP sessions from the quota that are in use.
Session	The number of NAT sessions.
Pool	Name of the pool from which the public address for the session was selected.
LID	Limit ID (LID) in which the user quota is configured.
Flag	Displays a “U” if the quota is unusable.

show cgnv6 fixed-nat alg

Description Show Application Level Gateway (ALG) statistics for Fixed-NAT.

Syntax

```
show cgnv6 fixed-nat alg
{esp | ftp | h323 | mgcp | pptp | rtsp | sip | tftp}
statistics
```

Specify one of the protocols to see statistics for that protocol:

Parameter	Description
esp	Encapsulating Security Payload (ESP)
ftp	File Transfer Protocol (FTP).
h323	H.323 standard.
mgcp	Media Gateway Control Protocol
pptp	Point-to-Point Tunneling Protocol (PPTP) Generic Routing Encapsulation (GRE)
rtsp	Real Time Streaming Protocol (RTSP)

Parameter	Description
sip	Session Initiation Protocol (SIP)
tftp	Trivial File Transfer Protocol (TFTP)

Mode All

Related Commands:

- show cgnv6 lsn alg

show cgnv6 fixed-nat full-cone-sessions

Description Show Fixed-NAT full-cone sessions.

Syntax

```
show cgnv6 fixed-nat full-cone-sessions
[ds-lite [nat-address ipaddr] |
 nat-address ipaddr |
 nat44 [nat-address ipaddr] |
 nat64 [nat-address ipaddr] ]
[all-partitions | partition name]
[pcp]
```

Parameter	Description
ds-lite [**nat-address** *ipaddr*]	Displays DS-Lite full-cone sessions.
nat-address *ipaddr*	Displays full-cone sessions for the specified NAT address.
nat44 [**nat-address** *ipaddr*]	Displays NAT44 full-cone sessions.
nat64 [**nat-address** *ipaddr*]	Displays NAT64 full-cone sessions.
all-partitions	Displays full-cone sessions for all partitions.
partition *name*	Displays full-cone sessions for only the specified partition.
pcp	Displays only those full-cone sessions created by PCP request.

Mode All

show cgnv6 fixed-nat histogram

Description Show a histogram of active TCP or UDP users using ports in specific port ranges.

Syntax

```
show cgnv6 fixed-nat histogram
[port usage {inside-user | nat ip}
```

Parameter	Description
inside user	Displays a histogram of active TCP or UDP users using ports in specific port ranges as defined in the configuration to which the inside user belongs.
nat ip	Displays a histogram of active TCP or UDP users using ports in specific port ranges as defined in the configuration to which the NAT IP belongs.

Mode All

show cgnv6 fixed-nat inside-user

Description Show Fixed-NAT information for a specific inside client.

Syntax

```
show cgnv6 fixed-nat inside-user {ipv4addr | ipv6addr}
[partition name]
{port-mapping | quota-used}
```

Parameter	Description
partition *name*	Name of the inside user partition.
port-mapping	Displays Fixed-NAT port mappings for a specific NAT address.
quota-used	Lists the number of sessions the client currently has active, and the number of TCP, UDP, and ICMP ports in use by the client.

Mode All

show cgnv6 fixed-nat nat-address

Description Display Fixed-NAT address information.

Syntax

```
show cgnv6 fixed-nat nat-address ipv4addr
{portnum | port-mapping}
```

Parameter	Description
portnum	Displays the inside user mapping for NAT address and NAT port number (1024-65535).
port-mapping	Displays Fixed-NAT port mappings for a specific NAT address.

Mode All

show cgnv6 fixed-nat port-mapping-files

Description Display all created files currently on the file system.

Syntax

```
show cgnv6 fixed-nat port-mapping-files {all | archive}
```

Parameter	Description
all	List all the port mapping files of all configuration
archive	List all the port mapping files that are deleted.

Mode All

Example This show a sample output:

```
ACOS(config)# show cgnv6 fixed-nat port-mapping-files
Fixed Nat Port Mapping Files
-----------------------------------------------------
fixed_nat_150.150.150.150
Total: 1
```

show cgnv6 fixed-nat statistics

Description Show statistics for Fixed-NAT.

Syntax

```
show cgnv6 fixed-nat statistics
```

Mode All

The following table describes the fields in this command's output.

Field	Description
Total NAT Addresses in-use	Total number of NAT pool addresses in use.
Total TCP Ports Allocated	Total number of TCP ports allocated for user sessions.
Total TCP Ports Freed	Total number of TCP ports freed for use by other sessions.
Total UDP Ports Allocated	Total number of UDP ports allocated for user sessions.
Total UDP Ports Freed	Total number of UDP ports freed for use by other sessions.
Total ICMP Ports Allocated	Total number of ICMP ports allocated for user sessions.
Total ICMP Ports Freed	Total number of ICMP ports freed for use by other sessions.
NAT44 Data Sessions Created	Total number of NAT44 Fixed-NAT data sessions created.
NAT44 Data Sessions Freed	Total number of NAT44 Fixed-NAT data sessions freed.
NAT64 Data Sessions Created	Total number of NAT64 Fixed-NAT data sessions created.
NAT64 Data Sessions Freed	Total number of NAT64 Fixed-NAT data sessions freed.
DS-Lite Data Sessions Created	Total number of DS-Lite Fixed-NAT data sessions created.

Field	Description
DS-Lite Data Sessions Freed	Total number of DS-Lite Fixed-NAT data sessions freed.
TCP NAT Port Unavailable	Number of times a TCP port for an LSN NAT session was unavailable.
UDP NAT Port Unavailable	Number of times a UDP port for an LSN NAT session was unavailable.
ICMP NAT Port Unavailable	Number of times an ICMP port for an LSN NAT session was unavailable.
Sessions User Quota Exceeded	Number of times a client exceeded their data session quota.
NAT44 TCP Full-Cone Created	Total number of NAT44 TCP full-cone sessions created.
NAT44 TCP Full-Cone Freed	Total number of NAT44 TCP full-cone sessions freed.
NAT44 UDP Full-Cone Created	Total number of NAT44 UDP full-cone sessions created.
NAT44 UDP Full-Cone Freed	Total number of NAT44 UDP full-cone sessions freed.
NAT44 UDP ALG Full-Cone Created	Total number of NAT44 UDP full-cone sessions created that used ALG support.
NAT44 UDP ALG Full-Cone Freed	Total number of NAT44 UDP full-cone sessions freed that used ALG support.
NAT64 TCP Full-Cone Created	Total number of NAT64 TCP full-cone sessions created.
NAT64 TCP Full-Cone Freed	Total number of NAT64 TCP full-cone sessions freed.
NAT64 UDP Full-Cone Created	Total number of NAT64 UDP full-cone sessions created.
NAT64 UDP Full-Cone Freed	Total number of NAT64 UDP full-cone sessions freed.
NAT64 UDP ALG	Total number of NAT64 UDP full-cone sessions

Field	Description
Full-Cone Created	created that used ALG support.
NAT64 UDP ALG Full-Cone Freed	Total number of NAT64 UDP full-cone sessions freed that used ALG support.
DS-Lite TCP Full-Cone Created	Total number of DS-Lite UDP full-cone sessions created that used ALG support.
DS-Lite TCP Full-Cone Freed	Total number of DS-Lite UDP full-cone sessions freed that used ALG support.
DS-Lite UDP Full-Cone Created	Total number of DS-Lite TCP full-cone sessions created.
DS-Lite UDP Full-Cone Freed	Total number of DS-Lite TCP full-cone sessions freed.
DS-Lite UDP ALG Full-Cone Created	Total number of DS-Lite UDP full-cone sessions created.
DS-Lite UDP ALG Full-Cone Freed	Total number of DS-Lite UDP full-cone sessions freed.
Full-Cone Session Creation Failed	Total number of NAT64 UDP full-cone sessions created that used ALG support.
NAT44 Endpoint-Independent Mapping Matched	Total number of NAT64 UDP full-cone sessions freed that used ALG support.
NAT64 Endpoint-Independent Mapping Matched	Number of times the NAT64 mapping assigned to a client was reused for subsequent traffic for that client.
DS-Lite Endpoint-Independent Mapping Matched	Number of times the DS-Lite mapping assigned to a client was reused for subsequent traffic for that client.
NAT44 Endpoint-Independent Filtering Matched	Number of times traffic from any source to a given NAT44 mapped client was forwarded to the internal client, regardless of the endpoint. (This is the benefit provided by Endpoint independent filtering.)

Field	Description
NAT64 Endpoint-Independent Filtering Matched	Number of times traffic from any source to a given NAT64 mapped client was forwarded to the internal client, regardless of the endpoint.
DS-Lite Endpoint-Independent Filtering Matched	Number of times traffic from any source to a given DS-Lite mapped client was forwarded to the internal client, regardless of the endpoint.
NAT44Endpoint-Dependent Filtering Drop	Number of times traffic to a NAT44 mapped client was dropped because endpoint-independent filtering was not enabled, and the traffic was not from the endpoint mapped to the client.
NAT64Endpoint-Dependent Filtering Drop	Number of times traffic to a NAT64 mapped client was dropped because endpoint-independent filtering was not enabled, and the traffic was not from the endpoint mapped to the client.
DS-Lite Endpoint-Dependent Filtering Drop	Number of times traffic to a DS-Lite mapped client was dropped because endpoint-independent filtering was not enabled, and the traffic was not from the endpoint mapped to the client.
NAT44 Endpoint-Independent Filtering Inbound Limit Exceeded	Number of times the limit for EIF sessions on a NAT44 mapping was exceeded.
NAT64 Endpoint-Independent Filtering Inbound Limit Exceeded	Number of times the limit for EIF sessions on a NAT64 mapping was exceeded.
DS-Lite Endpoint-Independent Filtering Inbound Limit Exceeded	Number of times the limit for EIF sessions on a DS-Lite mapping was exceeded.

Field	Description
NAT44 Hairpin Session Created	Total number of NAT44 hairpin sessions created.
NAT64 Hairpin Session Created	Total number of NAT64 hairpin sessions created.
DS-Lite Hairpin Session Created	Total number of DS-Lite hairpin sessions created.
Fixed NAT LID Standby Drop	Number of packets dropped because the Fixed-NAT LID is in an HA group, and this ACOS device was the Standby for that HA group.
Self-Hairpinning Drop	Number of times traffic was dropped because the inside source and destination addresses were the same.
Fixed NAT IPv6 in IPv4 Packet Drop	Number of Packets dropped because it is a ipv6 packet encapsulated in IPv4 packet. Fixed NAT does not support 6rd / IPv6 in IPv4 packets.
Fixed NAT Dest Rule List Drop	Number of Packets dropped because the Drop was configured in Destination Rule List.
Fixed NAT Dest Rule List Pass-Through	Number of Packets passed through because the Pass-Through was configured in Destination Rule List.
Fixed NAT IPv4 User Marked Unusable	Number of Fixed NAT IPv4 users set to unusable state.
Fixed NAT IPv6 User Marked Unusable	Number of Fixed NAT IPv6 users set to unusable state.
Fixed NAT User Unusable Drop	Number of Packets dropped because the user is in unusable state.
Fixed NAT Dest Rules List Source NAT Drop	Number of Packets dropped because LSN Source NAT was configured in Fixed-NAT Dest Rule List.
Fixed NAT Config	Packets dropped due to configuration is not

Field	Description
not Found	found. This can occur when the configuration is being removed.
Fixed NAT IPD disabled	Fixed-NAT IP black-listed due to cgnv6 ddos-protection. Number of times traffic hits this Fixed NAT IP once it is black-listed.

show cgnv6 l4

Description Show counters for cgnv6 l4.

Syntax

```
show counters cgnv6 l4
```

Mode All

Usage Used to view the counter values of the cgnv6 l4.

Example The following is the output of show counters cgnv6 l4:

```
ACOS# show cgnv6 l4
No Forward Route for Session                0
No Reverse Route for Session
Out of Session Memory
TCP RST Sent
IPIP ICMP Echo Reply Sent
ICMP Administratively Filtered Sent
ICMP Host Unreachable Sent
0
ICMP Reply No Session Drop
IPIP Truncated Packet
IPv4 Source Not Valid Unicast
        0
IPv4 Destination Not Valid Unicast
IPv6 Source Not Valid Unicast
        0
IPv6 Destination Not Valid Unicast
Rate Drop reset
```

The following table describes the fields in the command's output.

Field	Description
No Forward Route for Session	Route look up failure for session forward direction.
No Reverse Route for Session	Route look up failure for session reverse direction.
Out of Session Memory	No memory could be allocated to a new session.
TCP RST Sent	Sent TCP reset back for TCP error.
IPIP ICMP Echo Reply Sent	Sent ICMP replay back via IPv4 in IPV6 tunnel.
ICMP Administratively Filtered Sent	Sent adminitratively prohibited by filtering ICMP for NAT drop (it can be configured by “cgnv6 lsn icmp...”).
ICMP Host Unreachable Sent	Sent ICMP host unreachable for NAT drop (it can be configured by “cgnv6 lsn icmp...”).
ICMP Reply No Session Drop	No sessions was found for ICMP reply.
IPIP Truncated Packet	The IP in IP packet was too short to parse.
IPv4 Source Not Valid Unicast	IPv4 source IP not a valid unicast IP.
IPv4 Destination Not Valid Unicast	IPv4 destination IP not a valid unicast IP.
IPv6 Source Not Valid Unicast	IPv6 source IP not a valid unicast IP.
IPv6 Destination Not Valid Unicast	IPv6 destination IP not a valid unicast IP.
Rate Drop reset	Total number of unknown connection reset dropped by rate limit.

show cgnv6 logging keywords

Description Show valid keywords for RFC 5424 custom messages.

Syntax

```
show cgnv6 logging keywords  feature event
```

Parameter	Description
feature	Specifies the feature, which can be one of the following: • **ds-lite** – Message strings for DS-Lite traffic. • **http-request-got** – Message strings for HTTP request logs. • **lsn** – Message strings for CGN traffic. • **nat64** – Message strings for NAT64 traffic. • **session-created** – Message strings for session creation. For more information about the message strings, see Custom Format Keywords. • **session-deleted** – Message strings for session deletion. For more information about the message strings, see Custom Format Keywords. • **sixrd-nat64** – Message strings for 6rd-NAT64 traffic.
event	Specifies the event type, which can be one of the following (depending on the feature): • **fixed-nat-allocated** • **fixed-nat-freed** • **fixed-nat-interim-update** • **port-allocated** • **port-batch-allocated** • **port-batch-freed** • **port-batch-v2-allocated** • **port-batch-v2-freed** • **port-batch-v2-interim-update** • **port-freed**

Mode All

Example The following example shows sample output for the `show cgnv6 logging keywords session_created` command:

```
ACOS(config)#show cgnv6 logging keywords session-created
$rule-name$                    Rule name
$proto-name$                   Protocol name
$proto-num$                    Protocol number
$fwd-tuple-type$               Forward tuple type
$fwd-tunnel$                   Forward tuple tunnel IP
$fwd-src-ip$                   Forward tuple source IP
$fwd-src-port$                 Forward tuple source port
$fwd-dst-tunnel$               Forward tuple destination tunnel
$fwd-dst-ip$                   Forward tuple destination IP
$fwd-dst-port$                 Forward tuple destination port
$rev-tuple-type$               Reverse tuple type
$rev-tunnel$                   Reverse tuple tunnel IP
$rev-src-ip$                   Reverse tuple source IP
$rev-src-port$                 Reverse tuple source port
$rev-dst-tunnel$               Reverse tuple destination tunnel
$rev-dst-ip$                   Reverse tuple destination IP
$rev-dst-port$                 Reverse tuple destination port
$sesn-start-time$              Session start time (only for
"format    custom")
$sesn-start-time-epoch$        Session start time epoch (only
for "format custom")
$radius-msisdn$                RADIUS attribute: MSISDN
$radius-imei$                  RADIUS attribute: IMEI
$radius-imsi$                  RADIUS attribute: IMSI
$radius-ctm1$                  RADIUS attribute: Custom1
$radius-ctm2$                  RADIUS attribute: Custom2
$radius-ctm3$                  RADIUS attribute: Custom3
$radius-ctm4$                  RADIUS attribute: Custom4
$radius-ctm5$                  RADIUS attribute: Custom5
$radius-ctm6$                  RADIUS attribute: Custom6
```

Example The following example shows sample output for the `show cgnv6 logging keywords session_deleted` command:

```
ACOS(config)#show cgnv6 logging keywords session-deleted
```

$rule-name$	Rule name
$proto-name$	Protocol name
$proto-num$	Protocol number
$fwd-tuple-type$	Forward tuple type
$fwd-tunnel$	Forward tuple tunnel IP
$fwd-src-ip$	Forward tuple source IP
$fwd-src-port$	Forward tuple source port
$fwd-dst-tunnel$	Forward tuple destination tunnel
$fwd-dst-ip$	Forward tuple destination IP
$fwd-dst-port$	Forward tuple destination port
$rev-tuple-type$	Reverse tuple type
$rev-tunnel$	Reverse tuple tunnel IP
$rev-src-ip$	Reverse tuple source IP
$rev-src-port$	Reverse tuple source port
$rev-dst-tunnel$	Reverse tuple destination tunnel
$rev-dst-ip$	Reverse tuple destination IP
$rev-dst-port$	Reverse tuple destination port
$req-byte$	Request byte count
$rsp-byte$	Response byte count
$sesn-dur$	Session duration
$sesn-fwd-byte$	Session forward byte count
$sesn-rev-byte$	Session reverse byte count
$sesn-start-time$	Session start time (only for "format custom")
$sesn-start-time-epoch$	Session start time epoch (only for "format custom")
$sesn-end-time$	Session end time (only for "format custom")
$sesn-end-time-epoch$	Session end time epoch (only for "format custom")
$radius-msisdn$	RADIUS attribute: MSISDN
$radius-imei$	RADIUS attribute: IMEI
$radius-imsi$	RADIUS attribute: IMSI
$radius-ctm1$	RADIUS attribute: Custom1
$radius-ctm2$	RADIUS attribute: Custom2
$radius-ctm3$	RADIUS attribute: Custom3
$radius-ctm4$	RADIUS attribute: Custom4
$radius-ctm5$	RADIUS attribute: Custom5

show cgnv6 logging source-address

Description Display all source-address logging statistics about the state of the source address port allocation.

Syntax `show cgnv6 logging source-address`

Default N/A

Mode All

Usage You can also specify source-address logging statistics for a specific template.

show cgnv6 logging statistics

Description Show statistics for external logging.

Syntax `show cgnv6 logging statistics`

Mode All

Example The following example shows the sample output for the show counters cgnv6 logging command:

```
ACOS(config)#show cgnv6 logging statistics
/cgnv6/logging
************************************
TCP Session Created
  0
TCP Session Deleted
  0
TCP Port Allocated
  0
TCP Port Freed
  0
TCP Port Batch Allocated
  0
TCP Port Batch Freed
  0
```

```
UDP Session Created
  0
UDP Session Deleted
  0
UDP Port Allocated
  0
UDP Port Freed
  0
UDP Port Batch Allocated
  0
UDP Port Batch Freed
  0
ICMP Session Created
  0
ICMP Session Deleted
  0
ICMP Resource Allocated
  0
ICMP Resource Freed
  0
ICMPV6 Session Created
  0
ICMPV6 Session Deleted
  0
ICMPV6 Resource Allocated
  0
ICMPV6 Resource Freed
  0
GRE Session Created
  0
GRE Session Deleted
  0
GRE Resource Allocated
  0
GRE Resource Freed
  0
ESP Session Created
  0
```

```
ESP Session Deleted
  0
ESP Resource Allocated
  0
ESP Resource Freed
  0
Fixed NAT Inside User Port Mapping
  0
Fixed NAT Periodic Configs Logged
  0
Fixed NAT Periodic Config Logs Sent
  0
Fixed NAT Disabled Configs Logged
  0
Fixed NAT Disabled Config Logs Sent
  0
Fixed NAT Interim Updated
  0
Enhanced User Log
  0
Log Packets Sent
  0
Log Packets Dropped
  0
TCP Connection Established
  0
TCP Connection Lost
  0
TCP Port Overloading Allocated
  0
TCP Port Overloading Freed
  0
UDP Port Overloading Allocated
  0
UDP Port Overloading Freed
  0
HTTP Request Logged
  0
```

```
Reduced Logs by Destination Protocol and Port
  0
TCP Port Batch Interim Updated
  0
UDP Port Batch Interim Updated
  0
iDDoS L3 Entry Created
  0
iDDoS L3 Entry Deleted
  0
iDDoS L4 Entry Created
  0
iDDoS L4 Entry Deleted
  0
```

show cgnv6 logging tcp-svr-status

Description Displays status information for the TCP connections to logging servers.

Syntax

```
show cgnv6 logging tcp-svr-status templatetemplate-name
```

Replace *template-name* with the name of the active logging template. (This is the template set as the default CGN logging template.)

Mode All

Example The following command displays the status of the ACOS device's TCP connections to syslog servers:

```
ACOS# show cgnv6 logging tcp-svr-status template cgn-log-tmplt
Server                  No. of TCP connections    Status
-------------------------------------------------------
LogSrv1                 15/15                      OK
LogSrv2                 13/15                      Retrying
LogSrv3                 15/15                      OK
LogSrv4                 15/15                      OK
```

The following table describes the fields in the command output.

Field	Description
Server	Name of the syslog server.
No. of TCP connections	Status of the TCP connections to the server. The status is shown as follows: *Established-Connections* / *Data-CPUs* To optimize performance, the ACOS device establishes a separate TCP session from each data CPU to each syslog server. The Established-Connections value is the number of connections that currently are established. The Data-CPUs value is the number of data CPUs on the ACOS device. This number varies depending on the ACOS model.
Status	Connection status: • OK – All ACOS TCP connections to the syslog server are functioning normally. • Retrying – Some connections are not up, and the ACOS device is sending SYNs to try to establish the missing connections.

show cgnv6 lsn alg

Description Show Application Level Gateway (ALG) information for LSN, NAT64, and DS-Lite.

Syntax

```
show cgnv6 lsn alg
{esp | ftp | h323 | mgcp | pptp | rtp-stun-timeout | rtsp |
sip | tftp}
{config | statistics [debug]}
```

Parameter	Description
esp |	Specifies the protocol:

Parameter	Description
ftp | **h323** | **mgcp** | **pptp** | **rtp-stun-timeout** | **rtsp** | **sip** | **tftp**	• **esp** – IPsec Encapsulating Security Payload (ESP) • **ftp** – File Transfer Protocol (FTP) • **h323** – H.323 standard is a legacy voice-over-IP (VoIP) protocol. • **mgcp** – Media Gateway Control Protocol (MGCP) • **pptp** – Point-to-Point Tunneling Protocol (PPTP) Generic Routing Encapsulation (GRE) • **rtp-stun-timeout** – Show RTP/RTCP STUN timeout configuration. • **rtsp** – Real Time Streaming Protocol (RTSP) • **sip** – Session Initiation Protocol (SIP) • **tftp** – Trivial File Transfer Protocol (TFTP)
config | **statistics** [**debug**]	Specifies the type of information to display: • config – Indicates whether LSN ALG support for the protocol is enabled. • **statistics** [**debug**] – Displays statistics for the protocol. The **debug** option displays additional statistics.

Mode All

Example The following commands show information for ESP ALG:

```
ACOS# show cgnv6 lsn alg esp statistics
LSN ESP ALG Statistics:
---------------------------
ESP Sessions Created                    2
```

The following commands show information for FTP ALG:

```
ACOS# show cgnv6 lsn alg ftp config
LSN ALG for FTP is enabled on port 21.
ACOS# show cgnv6 lsn alg ftp statistics
LSN FTP ALG Statistics:
---------------------------
```

```
PORT Requests From Client                0
EPRT Requests From Client                2
LPRT Requests From Client                0
PASV Replies From Server                 3
EPSV Replies From Server                 0
LPSV Replies From Server                 0
```

The following table describes the fields in the command's output.

Field	Description
PORT Requests From Client	Number of FTP PORT requests received from clients.
EPRT Requests From Client	Number of FTP EPRT requests received from clients.
LPRT Requests From Client	Number of FTP LPRT requests received from clients.
PASV Replies From Server	Number of passive mode replies received from servers.
EPSV Replies From Server	Number of EPSV replies received from servers.
LPSV Replies From Server	Number of LPSV replies received from servers.

Example The following command shows statistics for PPTP ALG:

```
ACOS# show cgnv6 lsn alg pptp statistics
LSN PPTP ALG Statistics:
---------------------------
Calls Established                        0
Mismatched PNS Call ID                   0
GRE Sessions Created                     0
GRE Sessions Freed                       0
No Matching GRE Session                  0
Call ID Mismatch on Call Request         0
Call ID Mismatch on Call Reply           0
```

The following table describes the command's output.

Field	Description
Calls Established	Number of PPTP call sessions created.
Mismatched PNS Call ID	Number of times PPTP call packets did not match the PNS call ID.
GRE Sessions Created	Number of PPTP GRE sessions created.
GRE Sessions Freed	Number of PPTP GRE sessions freed.
No Matching GRE Session	Number of times GRE packets did not match a GRE session.
Call ID Mismatch on Call Request	Number of call IDs not matching call requests
Call ID Mismatch on Call Reply	Number of call IDs not matching call replies.

Example The following command shows statistics for RTSP ALG:

```
ACOS# show cgnv6 lsn alg rtsp statistics
LSN RTSP ALG Statistics:
---------------------------
Streams Created                          0
Streams Freed                            0
Stream Creation Failures                  0
Stream Client Ports Allocated            0
Stream Client Ports Freed                0
Stream Client Port Allocation Failures   0
Server Replies With Unknown Client Ports 0
Data Session Created                     0
Data Session Freed                       0
Data Session Creation Failures           0
```

The following table describes the fields in the command's output.

Field	Description
Streams Created	Number of RTSP stream sessions created.
Streams Freed	Number of RTSP stream sessions freed.
Stream Creation Failures	Number of times creation of an RTSP stream failed because the ACOS device was out of

Field	Description
	memory for sessions.
Stream Client Ports Allocated	Number of NAT ports allocated to client for creating streams.
Stream Client Ports Freed	Number of NAT ports freed.
Stream Client Port Allocation Failures	Number of times port allocation for a stream failed.
Server Replies With Unknown Client Ports	Number of server replies to SETUP that were addressed to an unknown client port.
Data Session Created	Number of UDP data sessions created for streaming video.
Data Session Freed	Number of UDP data sessions freed.
Data Session Creation Failures	Number of times creation of a data session failed because the ACOS device was out of memory for sessions.

Example The following command shows statistics for SIP ALG:

```
ACOS# show cgnv6 lsn alg sip statistics
LSN SIP ALG Statistics:
---------------------------
SIP Method REGISTER                     544
SIP Method INVITE                       0
SIP Method ACK                          544
SIP Method CANCEL                       0
SIP Method BYE                          544
SIP Method OPTIONS                      100
SIP Method PRACK                        0
SIP Method SUBSCRIBE                    8
SIP Method NOTIFY                       10
SIP Method PUBLISH                      0
SIP Method INFO                         0
SIP Method REFER                        0
SIP Method MESSAGE                      0
SIP Method UPDATE                       0
```

```
SIP Method UNKNOWN                              0
```

The following table describes the fields in the command's output.

Field	Description
SIP Method REGISTER	Number of SIP REGISTER messages received by the ACOS device. **NOTE:** This counter and all the following counters in the output apply to messages both from User Agent Servers (UASs) and User Agent Clients (UACs).
SIP Method INVITE	Number of SIP INVITE messages received by the ACOS device.
SIP Method ACK	Number of SIP ACK messages received by the ACOS device.
SIP Method CANCEL	Number of SIP CANCEL messages received by the ACOS device.
SIP Method BYE	Number of SIP BYE messages received by the ACOS device.
SIP Method OPTIONS	Number of SIP OPTIONS messages received by the ACOS device.
SIP Method PRACK	Number of SIP PRACK messages received by the ACOS device.
SIP Method SUBSCRIBE	Number of SIP SUBSCRIBE messages received by the ACOS device.
SIP Method NOTIFY	Number of SIP NOTIFY messages received by the ACOS device.
SIP Method PUBLISH	Number of SIP PUBLISH messages received by the ACOS device.
SIP Method INFO	Number of SIP INFO messages received by the ACOS device.
SIP Method REFER	Number of SIP REFER messages received by the ACOS device.

Field	Description
SIP Method MESSAGE	Number of SIP MESSAGE messages received by the ACOS device.
SIP Method UPDATE	Number of SIP UPDATE messages received by the ACOS device.
SIP Method UNKNOWN	Number of SIP UNKNOWN messages received by the ACOS device.

Example The following command shows statistics for TFTP ALG:

```
ACOS# show cgnv6 lsn alg tftp statistics
LSN TFTP ALG Statistics:
--------------------------
TFTP Client Sessions Created              2
```

show cgnv6 lsn enhanced-user-tracking

Description Shows the enhanced user tracking information for LSN.

Syntax

```
show cgnv6 lsn enhanced-user-tracking
[all-partitions]
[inside-useripaddr]
[partitionpartition-name]
[poolpool-name]
```

Parameter	Description
all-partitions | **partition** *partition-name*	Displays session information for all partitions or for a particular partition.
inside-user *ipaddr*	Displays session information only for the specified user IP address.
pool *pool-name*	Displays session information only for the specified LSN NAT pool.

Mode All

Example The following command shows the enhanced user tracking information for LSN:

```
ACOS(config)#show cgnv6 lsn enhanced-user-tracking
LSN Enhanced User Tracking:
Inside Addr  NAT Addr  TCP Current  UDP Current  ICMP Current
Session Current  TCP Session Current  UDP Session Current  TCP
Peak  UDP Peak  ICMP Peak  Session Peak  Lifetime Sessions
Upload Packets  Upload Bytes  Download Packets  Download Bytes
 NAT Pool Name
------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------------
---------------
1.0.101.11   2.0.0.2   0            64           0
20               0                   20                   0
      256       0          20            23                  0
             0             0                0
lsn_pool_1
LSN Enhanced User Tracking Count: 1
```

Field	Description
Inside Address	The private, internal IP address.
NAT Address	The public IP address that is mapped to the internal IP address.
TCP Current	The current number of TCP connections per user.
UDP Current	The current number of UDP connections per user.
ICMP Current	The current number of ICMP connections per user.
Session Current	The current number of connections per session per user.
TCP Session Current	The current number of TCP connections per session per user.
UDP Session Current	The current number of UDP connections per session per user.
TCP Peak	The peak number of TCP connections per user.

Field	Description
UDP Peak	The peak number of UDP connections per user.
ICMP Peak	The peak number of ICMP connections per user.
Session Peak	The peak number of connections per session per user.
Lifetime Sessions	The total number of lifetime sessions.
Upload Packets	The total number of upstream packet count per session.
Upload Bytes	The total number of upstream byte count per session.
Download Packets	The total number of downstream packet count per session.
Download Bytes	The total number of downstream byte count per session.
NAT Pool Name	The NAT pool to which the IP address belongs.

show cgnv6 lsn full-cone-sessions

Description Show currently active LSN full-cone sessions.

Syntax

```
show cgnv6 lsn full-cone-sessions
[all-partitions]
[inside-user ipaddr]
[partition partition-name]
[pcp]
[pool pool-name]
```

Parameter	Description
all-partitions | **partition** *partition-name*	Displays full-cone sessions for all partitions or for a particular partition.
inside-user	Displays full-cone sessions only for the specified

Parameter	Description
ipaddr	user.
pcp	Displays full-cone sessions created by PCP requests.
pool *pool-name*	Displays only the full-cone sessions that use a public IP address from the specified LSN NAT pool.

Mode All

Example The following command shows currently active LSN full-cone sessions:

```
ACOS# show cgnv6 lsn full-cone-sessions
LSN Full-cone Sessions:
Prot Inside Address     NAT Address Outbnd Inbnd  Pool
    CPU Age    Flags
------------------------------------------------------------------
----------------------------
UDP  10.10.10.4:30251 19.19.19.104:30251 1  0    lsn_p1
   4   -      -
Total Full-cone Sessions: 1
```

The following table describes the fields in the command's output.

Field	Description
Information for Individual Sessions:	
Prot	Protocol of the session.
Inside Address	Private IP address of the client.
NAT Address	Public IP address mapped to the client's private IP address.
Outbnd	Number of active outbound EIM sessions.
Inbnd	Number of active inbound EIF sessions.
Pool	LSN NAT pool from which the public IP address was assigned.
CPU	ACOS CPU on which the session resides.

Field	Description
Age	Number of seconds the session has been in effect. The symbol '**-**' indicates that the session is active i.e., aging hasn't started yet. However, **X** indicates that the session is inactive, and will reject any new inbound data sessions matching the full cone session
Flags	Indicate that the full-cone session was created by traffic or PCP.

show cgnv6 lsn inside-user

Description Show session information for a specific LSN inside client.

Syntax

```
show cgnv6 lsn inside-user ipaddr
```

Replace *ipaddr* with the inside IP address of the user.

Mode All

Example The following command shows LSN session information for an LSN user:

```
ACOS# show cgnv6 lsn inside-user 10.10.10.4
LSN User-Quota Sessions:
Inside Address       NAT Address          ICMP   UDP    TCP
Session Pool             LID
------------------------------------------------------------------
----------------------------
10.10.10.4           19.19.19.104         0      1      0
1       lsn_p1           1
Total User-Quota Sessions Shown: 1

LSN Full-cone Sessions:
Prot Inside Address         NAT Address            Outbnd
Inbnd  Pool             CPU Age    Flags
------------------------------------------------------------------
----------------------------
UDP  10.10.10.4:30251       19.19.19.104:30251     1      0
  lsn_p1           4   -      -
Total Full-cone Sessions: 1
```

```
LSN Data Sessions:
Prot Forward Source Forward Dest Reverse Source Reverse Dest
Age    Hash Flags    Type
-----------------------------------------------------------------
----------------------------
Udp  10.10.10.4:30251       19.19.19.1:82
19.19.19.1:82          19.19.19.104:30251     300    4
NSe0f0r0 LSN
```

The following table describes the fields in the command's output.

Field	Description
LSN User-Quota Sessions	Refer show cgnv6 lsn user-quota-sessions.
LSN Full-Cone Sessions	Refer show cgnv6 lsn full-cone-sessions.
LSN Data Sessions	Lists the following data session information for the user: • Prot – Protocol of the session • Inside Address – IPv4 address and protocol port of the client • NAT Address – NAT address assigned to the client by CGN • Outbnd – Number of active outbound EIM sessions. • Inbnd – Number of active inbound EIF sessions. • Pool – LSN pool name • CPU Age – Number of seconds the session has been in effect • Flags – Indicate that the full-cone session was created by traffic or PCP.

show cgnv6 lsn nat-address

Description Show LSN sessions filtered by NAT address.

Syntax

```
show cgnv6 lsn nat-addressnataddr[nat-port natport]
```

Parameter	Description
nataddr	Specifies the NAT IP address.
natport	Specifies the NAT port.

Mode All

Example The following command shows LSN session information filtered by NAT address for user 9.9.9.78

```
ACOS# show cgnv6 lsn nat-address 9.9.9.78
Prot Forward Source Forward Dest Reverse Source Reverse Dest
 Age   Hash Flags  Type
-------------------------------------------------------------
----------------------------
Udp  90.135.166.203:1966  9.9.9.173:10000  9.9.9.173:10000
9.9.9.78:36976  300   2  NFe0f0r0 LSN
Udp  130.69.85.151:1964   9.9.9.173:10000  9.9.9.173:10000
9.9.9.78:9379   300   5  NFe0f0r0 LSN
Total Sessions:          2
```

Example The following command shows LSN session information filtered by NAT address user 9.9.9.78 and NAT port 9379

```
ACOS# show cgnv6 lsn nat-address 9.9.9.78 nat-port 9379
Prot Forward Source Forward Dest Reverse Source    Reverse
Dest    Age   Hash Flags  Type
-------------------------------------------------------------
----------------------------
Udp  130.69.85.151:1964   9.9.9.173:10000  9.9.9.173:10000
9.9.9.78:9379   300   5  NFe0f0r0 LSN
Total Sessions:          1
```

The following table describes the fields in this command's output.

Field	Description
Prot	Transport protocol.
Forward Source	Client IP address when connecting to a VIP. • For DNS sessions, the client's DNS transaction ID is shown instead of a protocol port number. • The output for connection-reuse sessions shows 0.0.0.0 for the forward source and forward destination addresses. • For source-IP persistent sessions, the value shown in the Forward Source column is a combination of the IP address and the port number. The first two bytes of the displayed value are the third and fourth octets of the client IP address. The last two bytes of the displayed value represent the client source port.
Forward Dest	VIP to which the client is connected.
Reverse Source	Real server's IP address. **NOTE:** If the ACOS device is functioning as a cache server (RAM caching), asterisks (*) in this field and the Reverse Dest field indicate that the ACOS device directly served the requested content to the client from the ACOS RAM cache. In this case, the session is actually between the client and the ACOS device rather than the real server.
Reverse Dest	IP address to which the real server responds.
Age	Number of seconds since the session started.
Hash	CPU ID.
Flags	Processing path for the traffic:

Field	Description
	• NF – Fast-path processing. • NS – Slow-path processing.
Type	Type of NAT traffic.

show cgnv6 lsn port-overloading config

Description Display the configured Port Overloading settings that are ready to be deployed.

Syntax

```
show cgnv6 lsn port-overloading config
```

Mode All

Example Here is an example of the output:

```
ACOS# show cgnv6 lsn port-overloading config
LSN Port-Overloading Configured:
cgnv6 lsn port-overloading unique destination-address-and-port
cgnv6 lsn port-overloading tcp enable 60000 to 61000
cgnv6 lsn port-overloading udp enable 60000 to 61000

LSN Port-Overloading Actual:
cgnv6 lsn port-overloading unique destination-address-and-port
cgnv6 lsn port-overloading tcp disable 1 to 59999
cgnv6 lsn port-overloading tcp enable 60000 to 61000
cgnv6 lsn port-overloading tcp disable 61001 to 65535
cgnv6 lsn port-overloading udp disable 1 to 59999
cgnv6 lsn port-overloading udp enable 60000 to 61000
cgnv6 lsn port-overloading udp disable 61001 to 65535
```

show cgnv6 lsn port-reservations

Description Show static LSN port reservations.

Syntax

```
show cgnv6 lsn port-reservations
```

Mode All

Example The following command shows static LSN port reservations:

```
ACOS# show cgnv6 lsn port-reservations
LSN Port Reservations
Inside Address                    Start    End      NAT Address
     Start    End
------------------------------------------------------------------
------------------------
192.168.1.1                       80       1024     203.0.113.1
     80       1024
Total Static Port Reservations: 1
```

The following table describes the fields in this command's output.

Field	Description
Inside Address	Inside client's IP address.
Start	Beginning protocol port number in the inside address' range.
End	Ending protocol port number in the inside address' range.
NAT Address	Public IP address assigned to the client by LSN.
Start	Beginning protocol port number that is statically mapped to the inside address' port range.
End	Ending protocol port number that is statically mapped to the inside address' port range.

show cgnv6 lsn statistics

Description Shows LSN statistics.

Syntax `show cgnv6 lsn statistics`

Mode All

Example The following command shows LSN statistics:

```
ACOS# show cgnv6 lsn statistics
Traffic statistics for LSN:
---------------------------
Total TCP Ports Allocated                0
Total TCP Ports Freed                    0
Total UDP Ports Allocated                0
Total UDP Ports Freed                    0
Total ICMP Ports Allocated               0
Total ICMP Ports Freed                   0
Data Session Created                     0
Data Session Freed                       0
User-Quota Created                       0
User-Quota Freed                         0
User-Quota Creation Failed               0
TCP NAT Port Unavailable                 0
UDP NAT Port Unavailable                 0
ICMP NAT Port Unavailable                0
New User NAT Resource Unavailable        0
TCP User-Quota Exceeded                  0
UDP User-Quota Exceeded                  0
ICMP User-Quota Exceeded                 0
Extended User-Quota Matched              0
Extended User-Quota Exceeded             0
Data Session User-Quota Exceeded         0
Conn Rate User-Quota Exceeded            0
TCP Full-cone Session Created            0
TCP Full-cone Session Freed              0
UDP Full-cone Session Created            0
UDP Full-cone Session Freed              0
Full-cone Session Creation Failed        0
Hairpin Session Created                  0
Self-Hairpinning Drop                    0
Endpoint-Independent Mapping Matched     0
Endpoint-Independent Filtering Matched   0
Endpoint-Dependent Filtering Drop        0
Endpoint-Independent Filtering Inbound Limit Exceeded 0
Port Overloading NAT Port TCP Created    0
Port Overloading NAT Port UDP Created    0
Port Overloading NAT Port TCP Freed      0
Port Overloading NAT Port UDP Freed      0
```

```
TCP Port Overloaded                          0
UDP Port Overloaded                          0
Port Overloading Attempt Failed              0
TCP Port Overloading Session Created         0
UDP Port Overloading Session Created         0
TCP Port Overloading Session Freed           0
UDP Port Overloading Session Freed           0
NAT Pool Unusable                            0
HA NAT Pool Unusable                         0
HA NAT Pool Batch Type Mismatch              0
No RADIUS Profile Match                      0
NAT IP TCP Max Ports Allocated               0
NAT IP UDP Max Ports Allocated               0
No Class-List Match                          0
LSN LID Drop                                 0
LSN LID Pass-through                         0
User-Quota Unusable Drop                     0
User-Quota Marked Unusable                   0
```

The following table describes the fields in this command's output.

Field	Description
Total TCP Ports Allocated	Total number of TCP ports allocated for user sessions.
Total TCP Ports Freed	Total number of TCP ports freed for use by other sessions.
Total UDP Ports Allocated	Total number of UDP ports allocated for user sessions.
Total UDP Ports Freed	Total number of UDP ports freed for use by other sessions.
Total ICMP Ports Allocated	Total number of ICMP ports allocated for user sessions.
Total ICMP Ports Freed	Total number of ICMP ports freed for use by other sessions.

Field	Description
Data Session Created	Total number of LSN data sessions created.
Data Session Freed	Total number of LSN data sessions freed.
User-Quota Created	Number of port mappings created for which the user quota had available mappings.
User-Quota Freed	Number of port mappings that were created for which the user quota had available mappings, that were later freed.
User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
TCP NAT Port Unavailable	Number of times a TCP port for an LSN NAT session was unavailable.
UDP NAT Port Unavailable	Number of times a UDP port for an LSN NAT session was unavailable.
ICMP NAT Port Unavailable	Number of times an ICMP port for an LSN NAT session was unavailable.
New User NAT Resource Unavailable	Number of times LSN resources (ICMP, TCP, or UDP) were not available for a new user.
TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
Extended User-Quota	Number of times the extended user quota was used to create a mapping.

Field	Description
Matched	
Extended User-Quota Exceeded	Number of times a NAT port was unavailable to a client because the client had exceeded the extended user quota.
Data Session User-Quota Exceeded	Number of times a client exceeded their data session quota.
Conn Rate User-Quota Exceeded	Number of times connection rate quota for a user was exceeded.
TCP Full-cone Session Created	Total number of LSN TCP full-cone sessions created.
TCP Full-cone Session Freed	Total number of LSN TCP full-cone sessions freed.
UDP Full-cone Session Created	Total number of LSN UDP full-cone sessions created.
UDP Full-cone Session Freed	Total number of LSN UDP full-cone sessions freed.
Full-cone Session Creation Failed	Number of times creation of a full-cone session failed.
Hairpin Session Created	Total number of LSN hairpin sessions created.
Self-Hairpinning Drop	Number of hairpin sessions dropped because the source and destination client were the same.
Endpoint-Independent	Number of times LSN reused the LSN mapping assigned to a client for subsequent traffic for that

Field	Description
Mapping Matched	client. (This is the benefit provided by Endpoint independent mapping.)
Endpoint-Independent Filtering Matched	Number of times traffic from any source to a given mapped client was forwarded to the internal client, regardless of the endpoint. (This is the benefit provided by Endpoint independent filtering.)
Endpoint-Dependent Filtering Drop	Number of times traffic to a mapped client was dropped because endpoint-independent filtering was not enabled, and the traffic was not from the endpoint mapped to the client.
Endpoint-Independent Filtering Inbound Limit Exceeded	Number of times the maximum number of Endpoint-Independent Filtering (EIF) sessions allowed for a NAT mapping was exceeded.
Port Over-loading NAT Port TCP Created	Number of times a TCP on an overloaded NAT port was created.
Port Over-loading NAT Port UDP Created	Number of times a UDP on an overloaded NAT port was created.
Port Over-loading NAT Port TCP Freed	Number of times a TCP created on an overloaded NAT port was freed.
Port Over-loading NAT Port UDP Freed	Number of times a UDP created on an overloaded NAT port was freed.
NAT Pool Mismatch	Number of times traffic was dropped because matching traffic for a current full-cone session or

Field	Description
Drop	user-quota session uses a different pool or pool group than the one redirected to by the rule list.
TCP Port Overloaded	Number of times a TCP port on a NAT address was assigned to a new client while another client was still using the mapping. Note: This counter and the other Port Overloading counters apply only if port overloading is configured.
UDP Port Overloaded	Number of times a UDP port on a NAT address was assigned to a new client while another client was still using the mapping.
Port Over-loading Attempt Failed	Number of times port overloading attempt failed.
TCP Port Overloading Session Created	Number of times a session on an overloaded TCP port was created.
UDP Port Overloading Session Created	Number of times a session on an overloaded UDP port was created.
TCP Port Overloading Session Freed	Number of times a session created on an overloaded TCP port was freed.
UDP Port Overloading Session Freed	Number of times a session created on an overloaded UDP port was freed.
NAT Pool Unusable	Number of times traffic hit a disabled NAT IP.
HA NAT Pool Unusable	Number of times traffic hit a disabled NAT IP in high availability standby state.

Field	Description
No RADIUS Profile Match	Number of times traffic did not match the RADIUS profile.
NAT IP TCP Max Ports Allocated	Number of times a NAT IP's all TCP ports have been allocated.
NAT IP UDP Max Ports Allocated	Number of times a NAT IP's all UDP ports have been allocated.
No Class-List Match	Number of times traffic did not match the LSN class list.
LSN LID Drop	Number of times traffic matched the drop action in the LSN LID, and was dropped.
LSN LID Pass-through	Number of times traffic matched the pass-through action in the LSN LID, and was passed through without being NATted.
User-Quota Unusable Drop	Number of times traffic was dropped because the user quota had been reached.
User-Quota Marked Unusable	Number of times traffic hit the user quota.

show cgnv6 lsn system-status

Description Show system-level information for LSN.

Syntax

```
show cgnv6 lsn system-status
```

Mode All

Example The following command shows system-level information for LSN:

```
ACOS# show cgnv6 lsn system-status
CPU Usage:
----------
Control CPU :  18%
Data CPU 1  :   0%
```

```
Data CPU 2  :   0%
Data CPU 3  :   0%
Data CPU 4  :   0%
Data CPU 5  :   0%
Data CPU avg:   0%

Memory Status:
--------------
Total Memory(KB): 6123184
Used Memory(KB) : 4462824
Free Memory(KB) : 1660360
Memory Usage    : 72.8%

Sessions Status:
----------------
LSN CPS           : 0
Data Sessions Used: 0
Data Sessions Free: 16744443
SMP Sessions Used : 0
SMP Sessions Free : 16580608

NAT Port Usage:
---------------
TCP NAT Ports Used: 0
TCP NAT Ports Free: 1290240
UDP NAT Ports Used: 0
UDP NAT Ports Free: 1290240

RADIUS Table Usage:
-------------------
RADIUS Entries Used: 0
RADIUS Entries Free: 1500000
```

The following table describes the fields in the command's output.

Field	Description
CPU Usage	Shows utilization for each CPU. The average utilization for all CPUs also is shown.
Memory	Shows memory usage information.

Field	Description
Status	
Sessions Status	Shows usage and availability for LSN traffic sessions. Date sessions are traffic sessions. SMP sessions are cross-CPU sessions.
NAT Port Usage	Shows current utilization information for Layer 4 NAT ports.
RADIUS Table Usage	Shows current utilization information for RADIUS table usage.

show cgnv6 lsn user-quota-sessions

Description Shows LSN user-quota session information.

Syntax

```
show cgnv6 lsn user-quota-sessions
[all-partitions]
[inside-useripaddr]
[partitionpartition-name]
[poolpool-name]
[topnum {all | icmp | tcp | udp}]
```

Parameter	Description
all-partitions | **partition** *partition-name*	Displays session information for all partitions or for a particular partition.
inside-user *ipaddr*	Displays session information only for the specified user IP address.
pool *pool-name*	Displays session information only for the specified LSN NAT pool.
top *num type*	Limits the display to the sessions with the highest counters for the specified resource type. You can specify 1-100.

Parameter	Description
	The resource type can be one of the following: • **all** – Displays the sessions with the highest counters for all resource types (ICMP, TCP, and UDP). • **icmp** – Displays the sessions with the highest counters for ICMP. • **tcp** – Displays the sessions with the highest counters for TCP. • **udp** – Displays the sessions with the highest counters for UDP.

Mode All

Example The following command shows user-quota information:

```
ACOS# show cgnv6 lsn user-quota-sessions
LSN User-Quota Sessions:
Inside Address   NAT Address     ICMP   UDP    TCP    Session
UDP Session TCP Session Pool      LID   Flag
------------------------------------------------------------------
----------------------
10.10.10.4       11.11.11.103    0      0      10     10
0           10                     lsn_p1    1      U
Total User-Quota Sessions: 1
```

Field	Description
Inside Address	Inside client's IP address.
NAT Address	Public IP address assigned to the client by LSN.
ICMP	Number of ICMP ports from the quota that are in use.
UDP	Number of UDP ports from the quota that are in use.
TCP	Number of TCP ports from the quota that are in use.

Field	Description
Session	Number of active sessions created by the client.
TCP Session	Number of TCP sessions from the quota that are in use.
UDP Session	Number of UDP sessions from the quota that are in use.
Pool	Name of the pool from which the public address for the session was selected.
LID	Limit ID (LID) in which the user quota is configured.
Flag	Displays a “U” if the quota is unusable.

show cgnv6 lsn-lid

Description Show configuration information for CGN Limit IDs (LIDs).

Syntax `show cgnv6 lsn-lid [num]`

Mode All

show cgnv6 lsn-rule-list

Description Show information for LSN rule lists.

Syntax `show cgnv6 lsn-rule-list list-name [domain-ip | statistics]`

Parameter	Description
list-name	Displays information for the specified CGN rule list.
domain-ip	Displays IPs for domain. For each rule in the list, the number of times traffic matched the rule (the number of “hits”) is listed.
statistics	Displays statistics. For each rule in the list, the number of times traffic matched the rule (the number of “hits”) is listed.

Mode All

Example The following command shows DNAT action statistics:

```
ACOS# show cgn lsn-rule-list 1 statistics
cgnv6 lsn-rule-list 1
 ip 7.7.7.101/32
  tcp port 0 action dnat domain 1.a10.com hits 0 domain-
unresolved-drops 0
  icmp action dnat domain 1.a10.com hits 2 domain-unresolved-
drops 0
 ip 7.7.7.104/32
  tcp port 0 action dnat domain 4.a10.com hits 0 domain-
unresolved-drops 0
  icmp action dnat domain 4.a10.com hits 4 domain-unresolved-
drops 4
```

The following table describes the counters in the command output:

Counter	Description
hits	Indicates the number of sessions that has hit the DNAT rule.
domain-unre-solved-drops	Indicates the number of sessions that has hit the DNAT rule but failed to apply DNAT action because there is no IP address resolved from this domain.

Example The following command shows DNAT action statistics:

```
ACOS# show cgn lsn-rule-list 1 statistics
cgnv6 lsn-rule-list 1
 ip 2.2.2.2/32
  default action dnat domain 1.a10.com hits 10 domain-
unresolved-drops
```

Example The following command shows some rule-list statistics:

```
ACOS# show cgn lsn-rule-list r1 statistics
cgnv6 lsn-rule-list r1
default
  tcp port 80 action snat pool lsn_p1 hits 1
  icmp action drop hits 4
```

show cgnv6 lw-4o6 binding-table

Description Show binding-table information for Lightweight 4over6.

Syntax

```
show cgnv6 lw-4o6 binding-table
[statistics [tunnel-address ipv6addr] | entries |files |
tunnel-address ipv6address [entries]]
```

Parameter	Description
entries	Lists binding table entries in the order that they are added either manually or from a file.
files	Lists the Lightweight 4over6 binding tables on the ACOS device, and their status.
statistics [tunnel-address ipv6addr]	Displays binding-table statistics.
tunnel-address *ipv6addr* [**entries**]	Displays information for the specified Lightweight 4over6 tunnel address.

Example Below is an example output for this command:

```
ACOS# show vrrp-a te-mac
VRID : 0
LW-4over6 Binding Table Name: lw_si
Tunnel IPv6 Address                          Public Address
Start Port   End Port     AFTR Tunnel IPv6 Address
------------------------------------------------------------------
--------------------
1000:107::11                                 1.0.107.11       1
        65535       1001:107::100
1000:108::22                                 1.0.108.22       1
        65535       1001:108::100
```

Mode All

show cgnv6 lw-4o6 binding-table-validation-log files

Description Show the validation log files resulting from the **lw-4o6 binding-table-validate** command. The maximum number of log files that can be present at any time is 100.

Syntax

```
show cgnv6 lw-4o6 binding-table-validation-log files
```

Mode All

Using the CLI

- To view all the binding table log files, enter the following command:

```
ACOS(config)# show cgnv6 lw-4o6 binding-table-validation-log
files
Binding Table Validation Log Files:
-----------------------------------
lw_si_1760466738
Total: 1 file(s)
```

It can also be used with the standard output modifiers:

```
ACOS# show cgnv6 lw-4o6 binding-table-validation-log files  |
?
  begin    Begin with the line that matches
  include  Include lines that match
  exclude  Exclude lines that match
  section  Filter a section of output
```

- To delete a binding table log file, enter the following command:

```
ACOS(config)# delete cgnv6 lw-4o6-binding-table-validation-log
<file-name>
```

- To export a binding table log file, enter the following command:

```
ACOS(config)# export lw-4o6-binding-table-validation-log
<file-name>
```

show cgnv6 lw-4o6 statistics

Description Show statistics for Lightweight 4over6.

Syntax `show cgnv6 lw-4o6 statistics`

Mode All

The following table describes the fields in this command's output.

Field	Description
Total Entries Configured	Total number of entries in the currently active binding table.
Self-Hairpinning Drops	Number of packets dropped because both the source and destination address information matched. • Both the source and destination IP addresses are the same, and match the IPv4 NAT address of any binding-table entry. For example: source IP address 10.10.10.100:x to destination IP address 10.10.10.100:y. • Both the source and destination IP addresses are the same and match a binding-table entry, and the packet's source and destination protocol ports also match the protocol port(s) of the same bridging-table entry. For example: source IP address 10.10.10.100:x to destination IP address 10.10.10.100:x. **NOTE:** Packets dropped for these reasons also are counted in the All Hairpinning Drops field (below).
All Hairpinning Drops	Number of packets dropped because both the source and destination IPv4 addresses matched entries in the binding table. This counter is incremented in any of the following cases: • The source IP address matches the IPv4 NAT address of any

Field	Description
	binding-table entry. • The destination IP address matches the IPv4 NAT address of any binding-table entry. • Any self-hairpinning drops occur.
No-Forward-Match ICMPv6 Sent	Number of times an ICMPv6 Destination Unreachable message was sent to a client CPE, because traffic from the client partially matched a binding-table entry but did not completely match any of the entries. For example, this counter is incremented if the ACOS device receives a packet whose IPv6 tunnel address does not match any binding-table entries. **NOTE:** This counter is incremented only if the feature is enabled.
No-Reverse-Match ICMP Sent	Number of times an IPv4 ICMP Destination Unreachable message was sent to an IPv4 server, because traffic from the server partially matched a binding-table entry but did not completely match any of the entries. **NOTE:** This counter is incremented only if the feature is enabled.
Inbound ICMP Drops	Number of inbound IPv4 ICMP packets that were dropped. **NOTE:** This counter is incremented only if the feature is enabled.
Forward Route Lookup Failed	Number of times client-to-server traffic was dropped because no route was available for forwarding it to the destination server.

Field	Description
Reverse Route Lookup Failed	Number of times server-to-client traffic was dropped because no route was available for forwarding it to the destination Lightweight 4over6 client.
LW-4over6 Interfaces not Configured Drops	Number of packets dropped due to LW-4over6 interfaces not being configured.
No Forward Binding Table Entry Match Drops	Number of packets dropped because no matching forward binding table entry was available.
No Reverse Binding Table Entry Match Drops	Number of packets dropped because no matching reverse binding table entry was available.

Related Commands:

- cgnv6 lw-4o6 no-forward-match
- cgnv6 lw-4o6 no-reverse-match
- cgnv6 lw-4o6 icmp-inbound

show cgnv6 map encapsulation domain

Description This command displays MAP-E domain configuration for all MAP-E domains, or for a specified MAP-E domain.

Syntax

```
show cgnv6 map encapsulation domain [domain-name]
```

Default N/A

Mode All

show cgnv6 map encapsulation statistics

Description This command displays MAP-E traffic statistics for all MAP-E domains, or for a specified MAP-E domain.

Syntax

```
show cgnv6 map encapsulation statistics [domain-name]
```

show cgnv6 map translation domain

Description This command displays MAP-T domain configuration for all MAP-T domains, or for a specified MAP-T domain.

Syntax

```
show cgnv6 map translation domain [domain-name]
```

Default N/A

Mode All

show cgnv6 map translation statistics

Description This command displays MAP-T traffic statistics for all MAP-T domains, or for a specified MAP-T domain.

Syntax

```
show cgnv6 map translation statistics [domain-name]
```

The show command output for all MAP-T traffic (no domain specified) is as follows:

```
MAP-T Statistics for domain 1:
--------------------------------
Inbound IPv4 Packets Received                       0
Inbound IPv4 Fragment Packets Received              0
Inbound IPv4 Destination Address Validation Failed 0
Inbound IPv4 Reverse Route Lookup Failed            0
Inbound IPv6 Destination Address Unreachable        0
Outbound IPv6 Packets Received                      0
Outbound IPv6 Fragment Packets Received             0
Outbound IPv6 Source Address Validation Failed      0
Outbound IPv6 Reverse Route Lookup Failed           0
Outbound IPv4 Destination Address Unreachable       0
```

```
Packet Exceeded MTU                                0
ICMP Packet Too Big Sent                           0
Interfaces not Configured Dropped                  0
BMR Prefix Rule Configured                         0
```

Default N/A

Mode All

show cgnv6 nat pool

Description Displays the configured NAT pools.

Syntax

```
show cgnv6 nat pool statistics[options] [pool-name] |
utilization
```

Parameter	Description
pool-name	Displays statistics for the specified CGN pool.
statistics *[options]*	Displays CGN pool statistics. The following filtering options are available: • *pool-name* – Name of a CGN pool. • **brief** – Displays fewer details. • **misc** – Displays miscellaneous per-IP information. • **peaks** – Displays peak statistics. • **top** *num suboption* – Limits the display to the pool IP addresses with the highest counters for the specified statistics type. You can specify 1-100. The statistics type can be one of the following: ◦ **used** – Displays the pool IP addresses with the highest total resource usage. ◦ **used-icmp** – Displays the pool IP addresses with the highest ICMP identifier usage.

Parameter	Description
	◦ **used-udp** – Displays the pool IP addresses with the highest UDP port usage. ◦ **used-tcp** – Displays the pool IP addresses with the highest TCP port usage. ◦ **reserved** – Displays the pool IP addresses with the most total reserved ports. ◦ **reserved-udp** – Displays the pool IP addresses with the most reserved UDP ports. ◦ **reserved-tcp** – Displays the pool IP addresses with the most reserved TCP ports. ◦ **users** – Displays the pool IP addresses with the most users.
utilization	Displays the CGNv6 NAT pool utilization statistics. This is applicable only to LSN.

Example The following command displays CGN NAT pool information:

```
ACOS# show cgnv6 nat pool
Total IP NAT Pools: 3
Pool Name            Start Address    End Address      Mask
Gateway          Vrid
------------------------------------------------------------------
----------------------------
test-lsn-pool        100.101.1.1      100.101.1.12     /24
0.0.0.0         default
```

The following table describes the fields in the command's output.

Field	Description
Pool Name	Name of the pool.
Start Address	Starting address of the pool.
End Address	Ending address of the pool.
Mask	Network mask for the pool address range.
Gateway	Default gateway to use for outbound client traffic mapped to an address from this pool.
VRID	VRRP-A VRID to which this pool is assigned, if applicable.

Example The following command shows LSN pool statistics:

```
ACOS# show cgnv6 nat pool Statistics
LSN Address Pool Statistics:
----------------------------
Pool Name Total IPs Total Users Free IPs Used IPs UDP-port-
overloaded TCP-port-overloaded
------------------- ----------------------------------------
-------------------------
pool1       10          4         6        4         5
           1


----------------------------
pool1   Address         Users ICMP Freed Total UDP Freed Total Rsvd
oLoaded TCP Freed Total Rsvd oLoaded
------------------------------------------------------------------
-----------------------------------
       19.19.19.101 0     0    0     0      0    0    0     0
    0     0    0    0     0    0
       19.19.19.102 0     0    0     0      0    0    0     0
    0     0    0    0     0    0
       19.19.19.103 1     0    0     0      1    0    1     0
    0     0    0    0     0    0
       19.19.19.104 0     0    0     0      0    0    0     0
    0     0    0    0     0    0
```

```
    19.19.19.105 1      0     0     0      0     0     0     0
3      0     0     0      0     1
    19.19.19.106 0      0     0     0      0     0     0     0
0      0     0     0      0     0
    19.19.19.107 1      0     0     0      0     0     0     0
0      0     0     0      0     0
    19.19.19.108 0      0     0     0      0     0     0     0
0      0     0     0      0     0
    19.19.19.109 0      0     0     0      0     0     0     0
0      1     1     0      0     0
    19.19.19.110 1      0     0     0      0     0     0     0
2      0     0     0      0     0
```

The following table describes the fields in this command's output.

Field	Description
Address	NAT (global) IP address.
Users	Number of inside IP addresses currently using the NAT IP address.
ICMP	Number of ICMP identifiers currently in use.
Freed (ICMP)	Total number of ICMP identifiers freed.
Total (ICMP)	Total number of ICMP identifiers allocated. ICMP column + Freed column = Total column.
UDP	Number of UDP ports currently in use.
Freed (UDP)	Total number of UDP ports freed.
Total (UDP)	Total number of UDP ports allocated. UDP column + Freed column = Total column.
Rsvd (UDP)	Total of all UDP reserve settings for each user that is currently using the NAT IP address. For example, if an LID has the setting "user-quota udp 100 reserve 50", and there are 50 users using the LID d on the NAT IP address, the Rsvd value is 50*50 = 2500.

Field	Description
oLoaded	Total number of UDP ports overloaded. **NOTE:** This counter and the other Port Overloading counters apply only if port overloading is configured.
TCP	Number of TCP ports currently in use.
Freed (TCP)	Total number of TCP ports freed.
Total (TCP)	Total number of TCP ports allocated. TCP column + Freed column = Total column.
Rsvd (TCP)	Total of all TCP reserve settings for each user that is currently using the NAT IP address. For example, if an LID has the setting “user-quota tcp 100 reserve 60”, and there are 10 users using the LID d on the NAT IP address, the Rsvd value is 10*60 = 600.
oLoaded	Total number of TCP ports overloaded. **NOTE:** This counter and the other Port Overloading counters apply only if port overloading is configured.

Example The following example shows use of the **misc** option:

```
ACOS# show cgnv6 nat pool statistics misc
LSN Address Pool Statistics:
-------------------------------------------------
lsn_p1           Address          ICMP     RTSP
-------------------------------------------------
                 19.19.19.101     0        0
                 19.19.19.102     0        0
                 19.19.19.103     0        0
                 19.19.19.104     0        0
                 19.19.19.105     0        0
                 19.19.19.106     0        0
                 19.19.19.107     0        0
                 19.19.19.108     0        0
```

```
                  19.19.19.109      0         0
                  19.19.19.110      0         0
```

Example The following example shows use of the **brief** option:

```
ACOS# show cgnv6 nat pool statistics brief
LSN Address Pool Statistics:
----------------------------
lsn_p1            Address           Users     UDP       TCP
----------------------------
                  19.19.19.101      0         0         0
                  19.19.19.102      0         0         0
                  19.19.19.103      1         1         0
                  19.19.19.104      0         0         0
                  19.19.19.105      0         0         0
                  19.19.19.106      0         0         0
                  19.19.19.107      0         0         0
                  19.19.19.108      0         0         0
                  19.19.19.109      0         0         0
                  19.19.19.110      0         0         0
```

Example The following command shows CGNv6 NAT pool utilization statistics. This is applicable only to LSN.

```
ACOS(config)#show cgnv6 nat pool utilization
NAT Pool Usage/Utilization Statistics:
----------------------------
Pool Name     Tot. TCP Port  Used TCP Port  TCP Usage %   Tot.
UDP Port  Used UDP Port  UDP Usage %   Users allowed  Current
Users  User Occ. %
------------------------------------------------------------------
------------------------------------------------------------------
----------------
nat_pool_1    16515072       129024         0
16515072       129024         0             1024           2

                              0
nat_pool_10   1032192        0              0
1032192        0              0             1032192        0

                              0
```

```
nat_pool_2    16515072        0               0
16515072        0               0             16515072        0

                                0
nat_pool_3    16515072        0               0
16515072        0               0             110080          0

                                0
nat_pool_4    1032192         0               0
1032192         0               0             1032192         0

                                0
nat_pool_5    1032192         0               0
1032192         0               0             1032192         0

                                0
nat_pool_7    1032192         0               0
1032192         0               0             0               0

                                0
-------------------------------------------------------------------
-------------------------------------------------------------------
-----------------
```

The following table describes the fields in this command's output.

Field	Description
Pool Name	Name of the pool.
Total TCP Port	Total number of TCP ports available for the pool.
Used TCP Port	Number of TCP ports used.
TCP Port Usage %	Percentage of TCP ports used.
Total UDP Port	Total number of UDP port available for the pool.
Used UDP Port	Number of UDP ports used.
UDP Port Usage %	Percentage of UDP ports used.

Field	Description
Users Allowed	Number of users allowed to use the NAT pool.
Current Users	Number of users currently using the NAT pool.
User Occupied %	Percentage of users using the NAT pool.

show cgnv6 nat pool-group

Description Display the configured NAT pool groups.

Syntax

```
show cgnv6 nat pool-groupgroup-name [statistics]
```

Example The following command shows the configuration of pool group “grp1”:

```
ACOS# show cgnv6 nat pool-group grp1
cgnv6 nat pool-group grp1
member test-lsn-pool
```

Parameter	Description
statistics	Displays NAT pool group statistics.

NOTE: To display the pool-group statistics for all pool groups, do not enter any pool group name.

Example The following command shows the configuration of all pool groups.

```
ACOS# show cgnv6 nat pool-group [statistics]
Pool Group Name      Total IP   Used IP    Free IP
-------------------------------------------------
grp2                 120        0          120
grp1                 145        0   To     145
-------------------------------------------------
```

show cgnv6 nat range-list

Description Display information on an IP source NAT static range list.

Syntax

```
[no] showcgnv6 nat range-list list-name
```

Default None.

Mode All

Example The following command displays information on an IP source NAT static range list:

```
ACOS# show cgnv6 nat range-list
Total Static NAT range lists: 1
Name    Local Address/Mask    Global Address/Mask    Count
VRID
-------------------------------------------------------------
--
abc     1.1.1.1/32            2.2.2.2/32              1       0
```

show cgnv6 nat static-binding

Description Display information on static bindings configured.

Syntax

```
[no] show cgnv6 nat static-binding
```

Default None.

Mode All

show cgnv6 nat46-stateless statistics

Description Show stateless NAT46 statistics.

Syntax

```
show cgnv6 nat46-stateless statistics
```

Mode All

Example The following command displays statistics for stateless NAT46:

```
ACOS(config)# show cgnv6 nat46-stateless statistics
Stateless NAT46 Statistics:
---------------------------
Outbound IPv4 packets received           10
Outbound IPv4 packets dropped            0
Outbound IPv4 fragment packets received  0
```

```
Outbound IPv6 destination unreachable    0
Outbound IPv6 packets fragmented         0
Inbound IPv6 packets received            101
Inbound IPv6 packets dropped             0
Inbound IPv6 fragment packets received   0
Inbound IPv4 destination unreachable     0
Inbound IPv4 packets fragmented          0
Packet too big                           0
Fragment process error                   0
ICMPv6 to ICMP                           1
ICMPv6 to ICMP error                     0
ICMP to ICMPv6                           0
ICMP to ICMPv6 error                     0
HA is standby                            0
Other errors                             0
```

The following table describes the fields in the command output.

Field	Description
Outbound IPv4 packets received	Number of client IPv4 packets received by the ACOS device.
Outbound IPv4 packets dropped	Number of client IPv4 packets dropped by the ACOS device.
Outbound IPv4 fragment packets received	Number of IPv4 packet fragments received from clients by the ACOS device.
Outbound IPv6 destination unreachable	Number of times the IPv6 destination was unreachable.
Outbound IPv6 packets fragmented	Number of outbound IPv6 packets fragmented.
Inbound IPv6 packets received	Number of inbound IPv6 packets received.
Inbound IPv6 packets dropped	Number of inbound IPv6 packets dropped.

Field	Description
Inbound IPv6 fragment packets received	Number of inbound fragmented IPv6 packets received.
Inbound IPv4 destination unreachable	Number of times the destination for inbound IPv4 traffic was unreachable.
Inbound IPv4 packets fragmented	Number of inbound IPv4 packets fragmented.
Packet too big	Number of oversize packets received.
Fragment processing errors	Number of fragment processing errors.
ICMPv6 to ICMP	Number of ICMPv6-to-ICMP translations.
ICMPv6 to ICMP errors	Number of ICMPv6-to-ICMP errors.
ICMP to ICMPv6	Number of ICMP-to-ICMPv6 translations.
ICMP to ICMPv6 errors	Number of ICMP-to-ICMPv6 errors.
HA is standby	Number of times the HA group the stateless NAT46 mappings are in was in the Standby state on this ACOS device.
Other errors	Number of errors other than those counted above.

show cgnv6 nat64 alg

Description Show Application Level Gateway (ALG) information for NAT64.

Syntax

```
show cgnv6 nat64 alg {esp | ftp | h323 | mgcp | pptp |rtsp | sip | tftp} config
```

Parameter	Description
esp	Shows whether NAT64 ALG support for Encapsulating

Parameter	Description
	Security Payload (ESP) is enabled.
ftp	Shows whether NAT64 ALG support for File Transfer Protocol (TFTP) is enabled.
h323	Shows whether NAT64 ALG support for H.323 standard is enabled.
mgcp	Shows whether NAT64 ALG support for Media Gateway Control Protocol (MGCP).
pptp	Shows whether NAT64 ALG support for Point-to-Point Tunneling Protocol (PPTP) is enabled.
rtsp	Shows whether NAT64 ALG support for Real Time Streaming Protocol (RTSP) is enabled.
sip	Shows whether NAT64 ALG support for Session Initiation Protocol (RTSP) is enabled.
tftp	Shows whether NAT64 ALG support for Trivial File Transfer Protocol (TFTP) is enabled.

Mode All

Usage The following command shows the NAT64 ALG state for RTSP:

```
ACOS# show cgnv6 nat64 alg rtsp config
NAT64 RTSP ALG is disabled on TCP port 554
```

show cgnv6 nat64 conversion

Description Show the IPv4 version of an IPv6 address or the IPv6 version of an IPv4 address.

Syntax

```
show cgnv6 nat64 conversion
{ipv4-addr | ipv6-addr}
prefix NAT64-prefix
```

Parameter	Description
ipv4-addr | *ipv6-addr*	Specifies the IP address to convert.

Parameter	Description
	• ipv4-addr – To display the IPv6 version of an IPv4 address, enter the IPv4 address. • ipv6-addr – To display the IPv4 version of an IPv6 address, enter the IPv4 address.
prefix *NAT64-prefix*	Specifies the NAT64 prefix to use for the conversion.

Mode All

Example The following command shows the IPv4 version of IPv6 address 64:ff9b::c0a8:10a, using the well-known NAT64 prefix (64:ff9b::/96):

```
ACOS# show cgnv6 nat64 conversion 64:ff9b::c0a8:10a prefix
64:ff9b::/96
Prefix: 64:ff9b::/96
IPv6: 64:ff9b::c0a8:10a
IPv4: 192.168.1.10
```

show cgnv6 nat64 enhanced-user-tracking

Description Shows the enhanced user tracking information for NAT64.

Syntax

```
show cgnv6 nat64 enhanced-user-tracking
[all-partitions]
[inside-useripaddr]
[partitionpartition-name]
[poolpool-name]
```

Parameter	Description
all-partitions | **partition** *partition-name*	Displays session information for all partitions or for a particular partition.

Parameter	Description
inside-user *ipaddr*	Displays session information only for the specified user IP address.
pool *pool-name*	Displays session information only for the specified LSN NAT pool.

Mode All

Example The following command shows the enhanced user tracking information for LSN:

```
ACOS(config)#show cgnv6 nat64 enhanced-user-tracking
NAT64 Enhanced User Tracking:
Inside IPv6   Prefix  NAT Address  TCP Current  UDP Current
ICMP Current  Session Current  TCP Session Current  UDP
Session Current  TCP Peak  UDP Peak  ICMP Peak  Session Peak
Lifetime Sessions  Upload Packets  Upload Bytes  Download
Packets  Download Bytes  NAT Pool Name
------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------------
----------------------------
1000:101::11  128     2.1.0.1      0            64           0
            20                0                     20
        0          64         0          20             23
         0                0             0                  0
          nat64_pool_1
NAT64 Enhanced User Tracking Count: 1
```

Field	Description
Inside IPv6	The private, internal IPV6 address.
Prefix	The user quota prefix configured for specified addresses.
NAT Address	The public IP address that is mapped to the internal IP address.
TCP Current	The current number of TCP connections per user.

Field	Description
UDP Current	The current number of UDP connections per user.
ICMP Current	The current number of ICMP connections per user.
Session Current	The current number of connections per session per user.
TCP Current	The current number of TCP connections per user.
UDP Current	The current number of UDP connections per user.
TCP Peak	The peak number of TCP connections per user.
UDP Peak	The peak number of UDP connections per user.
ICMP Peak	The peak number of ICMP connections per user.
Session Peak	The peak number of connections per session per user.
Lifetime Sessions	The total number of lifetime sessions.
Upload Packets	The total number of upstream packet count per session.
Upload Bytes	The total number of upstream byte count per session.
Download Packets	The total number of downstream packet count per session.
Download Bytes	The total number of downstream byte count per session.
NAT Pool Name	The NAT pool to which the IP address belongs.

show cgnv6 nat64 full-cone-sessions

Description Show currently active NAT64 full-cone sessions.

Syntax

```
show cgnv6 nat64 full-cone-sessions
[all-partitions]
[partition pool-name]
[pcp]
[pool pool-name]
```

Parameter	Description
all-partitions	Show full-cone sessions for all partitions
partition *partition-name*	Only show sessions from a specific partition.
pcp	Displays only the full-cone sessions that were created by a PCP request.
pool *pool-name* [**shared**]	Displays only the full-cone sessions that use a public IP address from the specified NAT pool.

Mode All

The following table describes the fields in this command's output.

Field	Description
Information for Individual Sessions:	
NAT Address	Public IPv4 or IPv6 address mapped to the client's private IPv6 address.
Conns	Number of connections currently using the session.
Pool	
CPU	ACOS CPU on which the session resides.
Age	Number of seconds the session has been in effect.
Statistics (brief option)	
NAT64 TCP Full-cone Session Created	Number of TCP full-cone sessions created.
NAT64 TCP Full-cone Session Freed	Number of TCP full-cone sessions freed.
NAT64 UDP Full-cone Session Created	Number of UDP full-cone sessions created.
NAT64 UDP Full-cone Session Freed	Number of UDP full-cone sessions freed.
NAT64 Full-cone Session Creation Failed	Number of times an attempt to create a NAT64 full-cone session failed.

show cgnv6 nat64 inside-user

Description Show session information for a specific NAT64 inside client.

Syntax

```
show cgnv6 nat64 inside-useripv6addr
```

Replace *ipv6addr* with the inside IPv6 address of the user.

Mode All

Example The following command shows session information for NAT64 user 2001:10::100:

```
ACOS# show cgnv6 nat64 inside-user 2001:10::100
NAT64 User-Quota Sessions:
Inside IPv6       NAT Address   ICMP   UDP    TCP    Pool
LID   Flag
------------------------------------------------------------------
--------
2001:10::100      172.7.7.30     0      2      2     lsn0    1
    U
Total User-Quota Sessions Shown: 1

NAT64 Full Cone Sessions:
Prot Inside IPv6
       NAT Address            Conns  Pool              CPU Age
------------------------------------------------------------------
----------------------------
UDP  [2001:10::100]:26635
       172.7.7.30:41995       1      lsn0               1   -
UDP  [2001:10::100]:64284
       172.7.7.30:48156       1      lsn0               4   -
TCP  [2001:10::100]:32063
       172.7.7.30:50239       1      lsn0               1   -
TCP  [2001:10::100]:32062
       172.7.7.30:25662       1      lsn0               2   -
Total Full Cone Sessions: 4
```

```
NAT64 Data Sessions:
Prot IP Type  IP Address and Port
                Age  Hash Flags
-----------------------------------------------------------------
----------------------------
Tcp  Fwd Src  [2001:10::100]:32063
                0    1    NS
     Fwd Dst  [64:ff9b::ac07:764]:80
     Rev Src  172.7.7.100:80
     Rev Dst  172.7.7.30:50239
Udp  Fwd Src  [2001:10::100]:26635
                300  1    NS
     Fwd Dst  [64:ff9b::ac07:764]:5300
     Rev Src  172.7.7.100:5300
     Rev Dst  172.7.7.30:41995
Tcp  Fwd Src  [2001:10::100]:32062
                0    2    NS
     Fwd Dst  [64:ff9b::ac07:764]:80
     Rev Src  172.7.7.100:80
     Rev Dst  172.7.7.30:25662
Udp  Fwd Src  [2001:10::100]:64284
                300  4    NS
     Fwd Dst  [64:ff9b::ac07:764]:5300
     Rev Src  172.7.7.100:5300
     Rev Dst  172.7.7.30:48156
```

The following table describes the fields in the command's output.

Field	Description
NAT64 User-Quota Sessions	Lists the following user-quota session information for the user: • Inside IPv6 – IPv6 address of the client • NAT Address – Client IPv4 NAT address from the LSN pool on the ACOS device • ICMP – Number of ICMP sessions from the quota that are in use

Field	Description
	• UDP – Number of UDP sessions from the quota that are in use • TCP – Number of TCP sessions from the quota that are in use • Pool – LSN NAT pool from which the NAT address for the session was selected • LID – Limit ID (LID) in which the user quota is configured
NAT64 Full-Cone Sessions	Lists the following information for the user's full-cone session: • Prot – Protocol of the session • Inside IPv6 – IPv6 address and protocol port of the client • NAT Address – Client IPv4 NAT address from the LSN pool on the ACOS device • Conns – Number of connections currently using the session • Pool – LSN NAT pool from which the NAT address for the session was selected • CPU – ACOS CPU on which the session resides • Age – Number of seconds the session has been in effect
NAT64 Data Sessions	Lists the following data session information for the user: • Prot – Protocol of the session • IP Type – Role of the IP address in the session: ◦ Fwd Src – IPv6 address and protocol port of the client ◦ Fwd Dst – Synthetic IPv6 address and

Field	Description
	protocol port of the server ◦ Rev Src – IPv4 address and protocol port of the server ◦ Rev Dst – Client IPv4 NAT address from the LSN pool on the ACOS device • IP Address and Port – IP addresses and protocol ports of the session • Age – Number of seconds the session has been in effect • Hash – Hash value for the session • Flags – This value is used by A10 Technical Support.

show cgnv6 nat64 nat-address

Description Show NAT64 sessions filtered by NAT address.

Syntax

```
show cgnv6 nat64 nat-address nataddr [nat-port natport]
```

Parameter	Description
nataddr	Specifies the NAT IP address.
natport	Specifies the NAT port.

Mode All

Example The following command shows NAT64 session information filtered by NAT address for user 9.9.9.75

```
ACOS# show cgnv6 nat64 nat-address 9.9.9.75
Prot IP Type  IP Address and Port
                Age  Hash Flags    Type
-----------------------------------------------------------------
-----------------------------------
```

```
Udp  Fwd Src  [3201::172]:34080
               240  1    NSe0f0r0 LSN
     Fwd Dst  [64:ff9b::909:9ad]:3000
     Rev Src  9.9.9.173:3000
     Rev Dst  9.9.9.75:62980
Udp  Fwd Src  [3201::172]:34861
               240  2    NSe0f0r0 LSN
     Fwd Dst  [64:ff9b::909:9ad]:3000
     Rev Src  9.9.9.173:3000
     Rev Dst  9.9.9.75:62990
Udp  Fwd Src  [3201::172]:35377
               240  3    NSe0f0r0 LSN
     Fwd Dst  [64:ff9b::909:9ad]:3000
     Rev Src  9.9.9.173:3000
     Rev Dst  9.9.9.75:62985
Total Sessions:          3
```

Example

The following command shows NAT64 session information filtered by NAT address user 9.9.9.75 and NAT port 62985.

```
ACOS# show cgnv6 nat64 nat-address 9.9.9.75 nat-port 62985
Prot IP Type  IP Address and Port Age  Hash Flags    Type
-------------------------------------------------------------------
-----
Udp  Fwd Src  [3201::172]:35377
               240  3    NSe0f0r0 LSN
     Fwd Dst  [64:ff9b::909:9ad]:3000
     Rev Src  9.9.9.173:3000
     Rev Dst  9.9.9.75:62985
Total Sessions:          1
```

The following table describes the fields in this sample output.

Field	Description
Prot	Layer 4 protocol of the session.
IP Type	The type of IP address: • Fwd Src - Forward Source • Fwd Dst - Forward Dest

Field	Description
	• Rev Src - Reverse Source • Rev Dst - Reverse Dest
IP Address and Port	IP address and port number for the corresponding IP Type
Age	Number of seconds since the session started.
Hash	CPU ID.
Flags	Processing path for the traffic: • NF – Fast-path processing. • NS – Slow-path processing.
Type	Type of NAT traffic.

show cgnv6 nat64 prefixes

Description Show the IPv6 prefixes configured for NAT64.

Syntax

```
show cgnv6 nat64 prefixes
```

Mode All

show cgnv6 nat64 statistics

Description Show statistics for NAT64.

Syntax

```
show cgnv6 nat64 statistics
```

Mode All

The following table describes the fields in this command's output.

Field	Description
Total TCP Ports Allocated	Total number of TCP ports allocated for user sessions.

Field	Description
Total TCP Ports Freed	Total number of TCP ports freed for use by other sessions.
Total UDP Ports Allocated	Total number of UDP ports allocated for user sessions.
Total UDP Ports Freed	Total number of UDP ports freed for use by other sessions.
Total ICMP Ports Allocated	Total number of ICMP ports allocated for user sessions.
Total ICMP Ports Freed	Total number of ICMP ports freed for use by other sessions.
Data Session Created	Total number of data sessions created.
Data Session Freed	Total number of data sessions freed.
User-Quota Created	Number of port mappings created for which the user quota had available mappings.
User-Quota Freed	Number of port mappings that were created for which the user quota had available mappings, that were later freed.
User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
TCP NAT Port Unavailable	Number of times a TCP port for an LSN NAT session was unavailable.
UDP NAT Port Unavailable	Number of times a UDP port for an LSN NAT session was unavailable.
ICMP NAT Port Unavailable	Number of times an ICMP port for an LSN NAT session was unavailable.

Field	Description
New User NAT Resource Unavailable	Number of times LSN resources (ICMP, TCP, or UDP) were not available for a new user.
TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
Extended User-Quota Matched	Number of times the extended user quota was used to create a mapping.
Extended User-Quota Exceeded	Number of times a NAT port was unavailable to a client because the client had exceeded the extended user quota.
Data Session User-Quota Exceeded	Number of times a client exceeded their data session quota.
Conn Rate User-Quota Exceeded	Number of times connection rate quota for a user was exceeded.
TCP Full-cone Session Created	Total number of LSN TCP full-cone sessions created.
TCP Full-cone Session Freed	Total number of LSN TCP full-cone sessions freed.
UDP Full-cone Session Created	Total number of LSN UDP full-cone sessions created.

Field	Description
UDP Full-cone Session Freed	Total number of LSN UDP full-cone sessions freed.
Full-cone Session Creation Failed	Number of times creation of a full-cone session failed.
Hairpin Session Created	Total number of LSN hairpin sessions created.
Self-Hairpinning Drop	Number of hairpin sessions dropped because the source and destination client were the same.
Endpoint-Independent Mapping Matched	Number of times LSN reused the LSN mapping assigned to a client for subsequent traffic for that client. (This is the benefit provided by Endpoint independent mapping.)
Endpoint-Independent Filtering Matched	Number of times traffic from any source to a given mapped client was forwarded to the internal client, regardless of the endpoint. (This is the benefit provided by Endpoint independent filtering.)
Endpoint-Dependent Filtering Drop	Number of times traffic to a mapped client was dropped because endpoint-independent filtering was not enabled, and the traffic was not from the endpoint mapped to the client.
Endpoint-Independent Filtering Inbound Limit Exceeded	Number of times the maximum number of Endpoint-Independent Filtering (EIF) sessions allowed for a NAT mapping was exceeded.
TCP Port Overloaded	Number of times a TCP port on a NAT address was assigned to a new client while another client was still using the mapping.

Field	Description
	Note: This counter and the other Port Overloading counters apply only if port overloading is configured.
UDP Port Overloaded	Number of times a UDP port on a NAT address was assigned to a new client while another client was still using the mapping.
TCP Port Overloading Session Created	Number of times a session on an overloaded TCP port was created.
UDP Port Overloading Session Created	Number of times a session on an overloaded UDP port was created.
TCP Port Overloading Session Freed	Number of times a session created on an overloaded TCP port was freed.
UDP Port Overloading Session Freed	Number of times a session created on an overloaded UDP port was freed.
NAT Pool Unusable	Number of times traffic hit a disabled NAT IP.
HA NAT Pool Unusable	Number of times traffic hit a disabled NAT IP in high availability standby state.
HA NAT Pool Batch Type Mismatch	Number of times traffic hit a mismatch of NAT pool batch type.
No RADIUS Profile Match	Number of times traffic did not match the RADIUS profile.
Layer 3 Forwarded Packets	Number of packets forwarded at Layer 3 because the IPv6 destination address did not match the NAT64 prefix.

Field	Description
Source Address Prefix Match Drop	Number of times incoming traffic matched the NAT64 prefix, but was dropped because it matched the drop action in the LSN-LID.
LSN LID Drop	Number of times traffic matched the drop action in the LSN LID, and was dropped.
LSN LID Pass-through	Number of times traffic matched the pass-through action in the LSN LID, and was passed through without being NATted.
No Class-List Match	Number of times traffic did not match the LSN class list.

show cgnv6 nat64 user-quota-sessions

Description Shows NAT64 user-quota session information.

Syntax

```
show cgnv6 nat64 user-quota-sessions
[all-partitions]
[partition partition-name]
[pool pool-name]
[prefix ipv6addr/prefix-length]
[top num {all | icmp | tcp | udp}]
```

Parameter	Description
all-partitions	Show users in all partitions.
partition *partition-name*	Sow users in a specific partition.
pool *pool-name*	Displays session information only for the specified NAT pool.
prefix *ipv6addr* **/***prefix-length*	Displays session information only for the specified IPv6 address(es).
top *num type*	Limits the display to the sessions with the highest counters for the specified resource type. You can specify 1-100.

Parameter	Description
	The resource type can be one of the following: • **all** – Displays the sessions with the highest counters for all resource types (ICMP, TCP, and UDP). • **icmp** – Displays the sessions with the highest counters for ICMP. • **tcp** – Displays the sessions with the highest counters for TCP. • **udp** – Displays the sessions with the highest counters for UDP.

Mode All

Example The following command shows user-quota information:

```
ACOS# show cgnv6 nat64 user-quota-sessions
NAT64 User-Quota Sessions:
Inside IPv6 Prefix  NAT Address ICMP UDP  TCP  Session
UDP Session TCP Session Pool      LID   Flag
------------------------------------------------------------------
---------------------
2001:20:20:20::75  128     10.2.0.111   0     1677  939  2616
   1677         939          p1    1    -
Total User-Quota Sessions: 1
```

The following table describes the fields in the command's output.

Field	Description
Information for Individual Sessions:	
Inside IPv6	Inside IP address of the client.
Prefix NAT Address	Public IP address assigned to the client.
ICMP	Number of ICMP sessions from the quota that are in use.

Field	Description
UDP	Number of UDP sessions from the quota that are in use.
TCP	Number of TCP sessions from the quota that are in use.
Session UDP	Number of UDP sessions from the quota that are in use.
Session TCP	Number of TCP sessions from the quota that are in use.
Session Pool	Name of the pool from which the public address for the session was selected.
LID	Limit ID (LID) in which the user quota is configured.
Flag	Displays a “U” if the quota is unusable.
Statistics (brief option)	
NAT64 User-Quota Created	Number of port mappings created for which the user quota had available mappings.
NAT64 User-Quota Freed	Number of port mappings that were created for which the user quota had available mappings, that were later freed.
NAT64 User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
NAT64 TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
NAT64 UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
NAT64 ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
NAT64 Extended	Number of times the extended user quota was

Field	Description
User-Quota Matched	used to create a mapping.
NAT64 Extended User-Quota Exceeded	Number of times a NAT port was unavailable to a client because the client had exceeded the extended user quota.
NAT64 Data Session User-Quota Exceeded	Number of times a client exceeded their data session quota.

show cgnv6 nptv6

Description Display the NPTv6 domains, or display statistics for NPTv6 domains.

Syntax `show cgnv6 nptv6 {domain | statistics} [domain-name]`

Mode All

Example The following example displays sample output:

```
ACOS(config)# show cgnv6 nptv6 statistics

NPTV6 Statistics for domain TEMP:
---------------------------------
Outbound Packets                                0
Inbound Packets                                 0
Haripin Packets                                 0
Address Not Valid For Translation               0
Inbound Packets No Map                          0
Packets Destination Unreachable                 0

NPTV6 Statistics for domain domain1:
---------------------------------
Outbound Packets                                0
Inbound Packets                                 0
Haripin Packets                                 0
Address Not Valid For Translation               0
Inbound Packets No Map                          0
```

```
Packets Destination Unreachable                    0
```

Usage The following table describes the fields for the show command output:

Field	Description
domain [*domain-name*]	Display all NPTv6 domains or a specific domain.
statistics [*domain-name*]	Display NPTv6 statistics for all domains or for a specific domain.

show cgnv6 one-to-one mappings

Description Display information on NAT one-to-one mappings.

Syntax

```
show cgnv6 one-to-one mappings
[all-partitions | partition partition-name]
[inside-address ipaddr]
[inside-address-ipv6 ipv6-addr]
[nat-addressipaddr]
[partition partition-name]
[poolpool-name [shared]]
```

Parameter	Description
all-partitions | **partition** *partition-name*	Displays mappings for all partitions or for a particular partition.
inside-address *ipaddr*	Displays information for a specific inside address.
inside-address-ipv6 ipv6-*addr*	Displays information for a specific IPv6 inside address.
nat-	Displays information for a specific NAT address.

Parameter	Description
ipaddr	
partition *partition-name*	Displays information for a specific partition.
pool *pool-name*	Displays mappings for a specific NAT pool. The **shared** option filters the output to include only pools that are configured to be shared with L3V partitions. This option is applicable when the command is entered from the shared partition, and displays mappings for pools that are configured in the shared partition and that are enabled to be shared with L3V partitions.

Example The following command displays CGN one-one mappings:

```
ACOS(config)# show cgnv6 one-to-one mappings
Inside IPv4 Address  Inside IPv6 Address  NAT Address
Sessions        Age    Pool
-------------------------------------------------------------------
----------------------------
 -                   2001:db8::2:10       6.6.6.6
9               -      p5
Total One-to-One NAT Mappings: 1
```

The following table describes the fields in the command's output.

Field	Description
Inside IPv4 Address	IPv4 inside address.
Inside IPv6 Address	IPv6 inside address
NAT Address	Public IP address assigned to the client by LSN.
Sessions	Number of sessions using this mapping.
Age	Age of this mapping.
Pool	Name of the pool.

show cgnv6 one-to-one pool

Description Display information on NAT one-to-one pool.

Syntax

```
show cgnv6 one-to-one pool [pool-name]
```

Parameter	Description
pool [*pool-name*]	Displays the name of the pool.
statistics	Displays the one-to-one NAT pool usage.

show cgnv6 one-to-one pool-group

Description Display the information on NAT one-to-one pool group.

Syntax

```
show cgnv6 one-to-one pool-group [pool-group-name]
```

show cgnv6 one-to-one statistics

Description Display information on NAT one-to-one statistics.

Syntax

```
show cgnv6 one-to-one statistics
```

Example To display one-to-one statistics, enter the following commands:

```
ACOS# show cgnv6 one-to-one statistics
Total One-to-One Mapping Allocated: 23456
Total One-to-One Mapping Freed: 23000
One-to-One Mapping Allocation Failure: 100
```

show cgnv6 pcp statistics

Description Show statistics for Port Control Protocol (PCP).

Syntax

```
show cgnv6 pcp statistics
```

Mode All

Example The following command shows PCP statistics:

```
ACOS# show cgnv6 pcp statistics
PCP Statistics:
---------------
Packets Received                                    0
PCP MAP Request Processing Success (NAT44)          0
PCP MAP Request Processing Success (DS-Lite)        0
PCP MAP Request Processing Success (NAT64)          0
PCP PEER Request Processing Success (NAT44)         0
PCP PEER Request Processing Success (DS-Lite)       0
PCP PEER Request Processing Success (NAT64)         0
PCP ANNOUNCE Request Processing Success (NAT44)     0
PCP ANNOUNCE Request Processing Success (DS-Lite)   0
PCP ANNOUNCE Request Processing Success (NAT64)     0
Packet Not a PCP Request                            0
Packet Too Short                                    0
Response No Route                                   0
Unsupported PCP version                             0
PCP Request Not Authorized                          0
PCP Request Malformed                               0
Unsupported PCP Opcode                              0
Unsupported PCP Option                              0
PCP Option Malformed                                0
No System or NAT Resources                          0
Unsupported Mapping Protocol                        0
User Quota Exceeded                                 0
Cannot Provide Suggested Port When PREFER_FAILURE   0
PCP Client Address Mismatch                         0
Excessive Remote Peers                              0
Packet Dropped For Not Coming From NAT Inside       0
L3/L4 Process Error                                 0
Internal Error                                      0
Unsolicited Announce Sent                           0
Unsolicited Announce Send Failure                   0
HA Sync PCP Epoch Sent                              0
HA Sync PCP Epoch Recv                              0
```

The following table describes the fields in the command's output.

Field	Description
Packets Received	Number of PCP request packets received by ACOS.
PCP MAP Request Processing Success (NAT44)	Number of NAT44 PCP MAP requests received and processed successfully by ACOS.
PCP MAP Request Processing Success (DS-Lite)	Number of DS-Lite PCP MAP requests received and processed successfully by ACOS.
PCP MAP Request Processing Success (NAT64)	Number of NAT64 PCP MAP requests received and processed successfully by ACOS.
PCP PEER Request Processing Success (NAT44)	Number of NAT44 PCP PEER requests received and processed successfully by ACOS.
PCP PEER Request Processing Success (DS-Lite)	Number of DS-Lite PCP PEER requests received and processed successfully by ACOS.
PCP PEER Request Processing Success (NAT64)	Number of NAT64 PCP PEER requests received and processed successfully by ACOS.
PCP ANNOUNCE Request Processing Success (NAT44)	Number of NAT44 PCP ANNOUNCE requests received and processed successfully by ACOS.
PCP ANNOUNCE Request Processing	Number of DS-Lite PCP ANNOUNCE requests received and processed successfully by ACOS.

Field	Description
Success (DS-Lite)	
PCP ANNOUNCE Request Processing Success (NAT64)	Number of NAT64 PCP ANNOUNCE requests received and processed successfully by ACOS.
Packet Not a PCP Request	Number of packets which are not a PCP request (e.g. PCP response).
Packet Too Short	Number of packets which are too short to be a valid PCP packet.
Response No Route	Number of packets for which ACOS cannot find the route on which to send back the PCP response.
Unsupported PCP version	Number of packets using a PCP protocol version which ACOS does not support.
PCP Request Not Authorized	Number of PCP requests sent from an unauthorized client.
PCP Request Malformed	Number of PCP requests which are malformed.
Unsupported PCP Opcode	Number of PCP packets with an unsupported PCP Opcode in the request.
Unsupported PCP Option	Number of PCP packets with a mandatory PCP Opcode in the request that is not supported by ACOS.
PCP Option Malformed	Number of PCP packs with malformed PCP options in the request.
No System or NAT Resources	Number of PCP requests for which ACOS cannot allocate a NAT port due to lack of available NAT ports or other system resources.
Unsupported Mapping Protocol	Number of packets for which the request port mapping is for a protocol other than TCP/UDP.

Field	Description
User Quota Exceeded	Number of packets for which ACOS cannot allocate a NAT port due to an exceeded user quota for the client.
Cannot Provide Suggested Port When PREFER_ FAILURE	Number of packets for which ACOS cannot allocate the suggested NAT port for PCP requests with a PREFER_FAILURE option.
PCP Client Address Mismatch	Number of packets for which the client address in the PCP payload is different from the source address of the PCP packet.
Excessive Remote Peers	Number of packets in which the PCP MAP request contains too many filters for remote peers.
Packet Dropped For Not Coming From NAT Inside	Number of PCP requests which are received from an ACOS interface but are not permitted by the ACOS configuration because they do not come from a NAT inside interface.
L3/L4 Process Error	Number of PCP packets which contain an error in the L3/L4 headers.
Internal Error	Number of unexpected internal errors from ACOS.
Unsolicited Announce Sent	Number of Unsolicited PCP Announce packets sent by ACOS.
Unsolicited Announce Send Failure	Number of times ACOS fails to send an Unsolicited PCP Announce packets.
HA Sync PCP Epoch Sent	For an HA Active box, the number of PCP epoch sync messages sent to a Standby box
HA Sync PCP Epoch Recv	For an HA Standby box, the number of PCP epoch sync messages received from the Active box.

show cgnv6 resource-usage

Description Display CGNv6 resource usage.

Syntax

```
show cgnv6 resource-usage
```

Example The following is the sample output of this command:

```
AX5100(config)# show cgnv6 resource-usage
Resource                          Current    Default    Minimum
   Maximum
------------------------------------------------------------------
------------
lsn-nat-addr-count                2048       2048       512
   10240
fixed-nat-ip-addr-count           128000     128000     2560
   128000
fixed-nat-inside-user-count       4000000    4000000    80000
   4000000
radius-table-size                 6000000    6000000    3000000
   6000000
```

show cgnv6 sixrd statistics

Description Show 6rd statistics.

Syntax

```
show cgnv6 sixrd statistics [domain-name]
```

Mode All

Example The following command displays statistics for the 6rd domain “6rd1”:

```
ACOS(config 6rd)#show cgnv6 sixrd statistics 6rd1
6rd Statistics for domain 6rd1:
----------------------------
Outbound TCP packets received             65
Outbound UDP packets received             13
Outbound ICMP packets received            10
Outbound other packets received           0
Outbound packets dropped                  0
Outbound IPv6 destination unreachable     1
```

```
Outbound Fragmented IPv6                    0
Inbound TCP packets received                66
Inbound UDP packets received                12
Inbound ICMP packets received               10
Inbound other packets received              0
Inbound packets dropped                     0
Inbound IPv4 destination unreachable        0
Inbound Fragmented IPv4                     0
Inbound Fragmented IPv6 in tunnel           0
Unknown 6rd delegated prefix                0
Packet too big                              0
Not local IP                                0
Fragment processing errors                  0
Other errors                                0
```

The following table describes the fields in this command's output.

Field	Description
Outbound TCP packets received	Number of client-to-server TCP packets received from clients.
Outbound UDP packets received	Number of client-to-server UDP packets received from clients.
Outbound ICMP packets received	Number of client-to-server ICMP packets received from clients.
Outbound other packets received	Number of fragmented client-to-server packets received from clients.
Outbound packets dropped	Number of client-to-server packets dropped by the ACOS device because they were larger than the MTU of the outgoing interface.
Outbound IPv6 destination unreachable	Number of client-to-server packets that could not be delivered because the IPv6 server was unreachable.

Field	Description
Outbound Fragmented IPv6	Number of client-to-server IPv6 packets that were fragmented by the ACOS device because they were larger than the MTU on the outgoing interface.
Inbound TCP packets received	Number of server-to-client TCP packets received from clients.
Inbound UDP packets received	Number of server-to-client UDP packets received from clients.
Inbound ICMP packets received	Number of server-to-client ICMP packets received from clients.
Inbound other packets received	Number of fragmented server-to-client packets received from clients.
Inbound packets dropped	Number of server-to-client packets dropped by the ACOS device because they were larger than the MTU of the outgoing interface.
Inbound IPv4 destination unreachable	Number of server-to-client packets that could not reach the destination of the IPv4 tunnel.
Inbound Fragmented IPv4	Number server-to-client packets fragmented into multiple IPv4 packets.
Inbound Fragmented IPv6 in tunnel	Number server-to-client packets fragmented into multiple IPv6 packets before being sent in the IPv4 tunnel.
Unknown 6rd delegated prefix	Number of packets received that had an unknown 6rd delegated prefix.
Packet too big	Number of packets received by the ACOS device from clients or servers that were larger than the

Field	Description
	MTU of the ACOS interface. This includes the following types of packets: • Inbound IPv6 packets from servers • Outbound IPv6 packets from 6rd clients
Not local IP	Number of times an inbound IPv6 packet matched a 6rd domain configuration, but the BR IPv4 address was a floating-IP address and its HA group on this ACOS device was in the standby state, so the IP address could not be used.
Fragment processing errors	Number of times the ACOS device could not process fragmented IPv4/IPv6 packets. For example, this counter is incremented if the fragment offset is not correct, or insufficient data is received, and so on.
Other errors	Number of other types of errors not covered by any of the counters above.

show cgnv6 template

Description Display CGN templates.

Syntax

```
show cgnv6 templates {dns | http-alg | logging | pcp | policy}
[template-name]
```

Default Use one of the options shown to specify the type of template to display.

show counters cgnv6 fixed-nat hw-accelerate

Description Display hardware forwarding statistics for fixed NAT sessions.

Syntax

```
show counters cgnv6 fixed-nat hw-accelerate
```

Example The following command displays information related to fixed NAT sessions accelerated to the hardware:

```
ACOS(config)# show counters cgnv6 fixed-nat hw-accelerate
```

```
show counters cgnv6 fixed-nat hw-accelerate
************************************
HW Entries Created                                  2
HW Entry Creation Failed                            0
HW Entry Creation Failed - server down              0
HW Entry Creation Failed - max entries exceeded     0
HW Entries Freed                                    2
HW Entries Freed - opposite tuple entry aged-out    1
HW Entry Freed - no HW prog                         0
HW Entry Freed - no matched conn                    0
HW Entry Freed - no software entry                  8
HW Entries Count                                    0
HW Entries Aged Out                                 8
HW Entries Aged Out - idle timeout                  8
HW Entries Aged Out - TCP FIN                       0
HW Entries Aged Out - TCP RST                       0
HW Entries Aged Out - invalid dst                   0
HW Entries Force HW Invalidate                      0
HW Entries Invalidate due to server down            0
TCAM Flows Created                                  1
TCAM Flows Freed                                    1
TCAM Flow Count                                     0
```

The following table describes the fields in the show command output.

Field	Description
HW Entries Created	Total number of hardware entries created.
HW Entry Creation Failed	Total number of times creation of hardware entries failed.
HW Entry Creation Failed - server down	Number of times creation of hardware entries failed since the server was down.
HW Entry Creation Failed - max entries exceeded	Number of times creation of hardware entries failed since the maximum entry count exceeded.
HW Entries Freed	Total number of hardware entries freed.
HW Entries Freed - opposite tuple entry	Number of hardware entries freed since the opposite tuple entry aged-out.

Field	Description
aged-out	
HW Entry Freed - no HW prog	Number of hardware entries freed since a hardware function was unavailable.
HW Entry Freed - no matched conn	Number of hardware entries freed since no connection matched.
HW Entry Freed - no software entry	Number of hardware entries freed since the software entry was not available.
HW Entries Count	Total number of hardware entries.
HW Entries Aged Out	Total number of hardware entries that aged-out.
HW Entries Aged Out - idle timeout	Number of hardware entries that aged-out due to idle timeout.
HW Entries Aged Out - TCP FIN	Number of hardware entries that aged-out after receiving a TCP FIN packet.
HW Entries Aged Out - TCP RST	Number of hardware entries that aged-out after receiving a TCP RST packet.
HW Entries Aged Out - invalid dst	Number of hardware entries that aged-out due to an invalid destination address.
HW Entries Force HW Invalidate	Number of hardware entries invalidated forcefully.
HW Entries Invalidate due to server down	Number of hardware entries invalidated since the server was down.
TCAM Flows Created	Total number of TCAM flows created.
TCAM Flows Freed	Total number of TCAM flows freed.
TCAM Flow Count	Total number of TCAM flows.

show counters cgnv6 fixed-nat per-instance

Description Display dynamic Fixed-NAT per VRID/User-Group counters. Each counter-block is differentiated by its key-name.

Syntax

```
show counters cgnv6 fixed-nat per-instance
```

NOTE: This command does not support filters.

Example The following command displays the counters:

```
key-name = fixed-nat-44-instance-0
/cgnv6/fixed-nat/per-instance

_____________________________________
Data Session Created 10
Data Session Freed 10
TCP Full-cone Session Created 0
TCP Full-cone Session Freed 0
UDP Full-cone Session Created 0
UDP Full-cone Session Freed 0
TCP Ports Allocated 0
TCP Ports Freed 0
UDP Ports Allocated 10
UDP Ports Freed 10
ICMP Ports Allocated 0
ICMP Ports Freed 0

_____________________________________
key-name = fixed-nat-64-instance-0
/cgnv6/fixed-nat/per-instance

_____________________________________
Data Session Created 0
Data Session Freed 0
TCP Full-cone Session Created 0
TCP Full-cone Session Freed 0
UDP Full-cone Session Created 0
UDP Full-cone Session Freed 0
TCP Ports Allocated 0
TCP Ports Freed 0
UDP Ports Allocated 0
UDP Ports Freed 0
ICMP Ports Allocated 0
ICMP Ports Freed 0

_____________________________________
key-name = fixed-nat-dslite-instance-0
/cgnv6/fixed-nat/per-instance

_____________________________________
Data Session Created 0
```

```
Data Session Freed 0
TCP Full-cone Session Created 0
TCP Full-cone Session Freed 0
UDP Full-cone Session Created 0
UDP Full-cone Session Freed 0
TCP Ports Allocated 0
TCP Ports Freed 0
UDP Ports Allocated 0
UDP Ports Freed 0
ICMP Ports Allocated 0
ICMP Ports Freed 0
```

The following table describes the fields in this command's output.

Field	Description
Data Session Created	Total number of LSN data sessions created for that instance.
Data Session Freed	Total number of LSN data sessions freed for that instance.
TCP Full-cone Session Created	Total number of LSN TCP full-cone sessions created for that instance.
TCP Full-cone Session Freed	Total number of LSN TCP full-cone sessions freed for that instance.
UDP Full-cone Session Created	Total number of LSN UDP full-cone sessions created for that instance.
UDP Full-cone Session Freed	Total number of LSN UDP full-cone sessions freed for that instance.
TCP Ports Allocated	Total number of TCP ports allocated for user sessions, for that instance.
TCP Ports Freed	Total number of TCP ports freed for use by other sessions, for that instance
UDP Ports Allocated	Total number of UDP ports allocated for user sessions, for that instance.
UDP Ports Freed	Total number of UDP ports freed for use by other sessions, for that instance.

Field	Description
ICMP Ports Allocated	Total number of ICMP ports allocated for user sessions, for that instance.
ICMP Ports Freed	Total number of ICMP ports freed for use by other sessions, for that instance.

show counters cgnv6 logging

Description Show statistics for external logging.

Syntax

```
show cgnv6 logging statistics
```

Mode All

Example The following example shows the sample output for the show counters cgnv6 logging command:

```
ACOS(config)#show counters cgnv6 logging
/cgnv6/logging
************************************
TCP Session Created
  0
TCP Session Deleted
  0
TCP Port Allocated
  0
TCP Port Freed
  0
TCP Port Batch Allocated
  0
TCP Port Batch Freed
  0
UDP Session Created
  0
UDP Session Deleted
  0
UDP Port Allocated
  0
```

```
UDP Port Freed
  0
UDP Port Batch Allocated
  0
UDP Port Batch Freed
  0
ICMP Session Created
  0
ICMP Session Deleted
  0
ICMP Resource Allocated
  0
ICMP Resource Freed
  0
ICMPV6 Session Created
  0
ICMPV6 Session Deleted
  0
ICMPV6 Resource Allocated
  0
ICMPV6 Resource Freed
  0
GRE Session Created
  0
GRE Session Deleted
  0
GRE Resource Allocated
  0
GRE Resource Freed
  0
ESP Session Created
  0
ESP Session Deleted
  0
ESP Resource Allocated
  0
ESP Resource Freed
  0
```

```
Fixed NAT Inside User Port Mapping
  0
Fixed NAT Periodic Configs Logged
  0
Fixed NAT Periodic Config Logs Sent
  0
Fixed NAT Disabled Configs Logged
  0
Fixed NAT Disabled Config Logs Sent
  0
Fixed NAT Interim Updated
  0
Enhanced User Log
  0
Log Packets Sent
  0
Log Packets Dropped
  0
TCP Connection Established
  0
TCP Connection Lost
  0
TCP Port Overloading Allocated
  0
TCP Port Overloading Freed
  0
UDP Port Overloading Allocated
  0
UDP Port Overloading Freed
  0
HTTP Request Logged
  0
Reduced Logs by Destination Protocol and Port
  0
TCP Port Batch Interim Updated
  0
UDP Port Batch Interim Updated
  0
```

```
iDDoS L3 Entry Created
  0
iDDoS L3 Entry Deleted
  0
iDDoS L4 Entry Created
  0
iDDoS L4 Entry Deleted
  0
```

show counters cgnv6 lsn hw-accelerate

Description Display hardware forwarding statistics for LSN (NAT44) sessions.

Syntax

```
show counters cgnv6 lsn hw-accelerate
```

Example The following command displays information related to LSN (NAT44) sessions accelerated to the hardware:

```
ACOS(config)# show counters cgnv6 lsn hw-accelerate
show counters cgnv6 lsn hw-accelerate
************************************
HW Entries Created                                  2
HW Entry Creation Failed                            0
HW Entry Creation Failed - server down              0
HW Entry Creation Failed - max entries exceeded     0
HW Entries Freed                                    2
HW Entries Freed - opposite tuple entry aged-out    1
HW Entry Freed - no HW prog                         0
HW Entry Freed - no matched conn                    0
HW Entry Freed - no software entry                  8
HW Entries Count                                    0
HW Entries Aged Out                                 8
HW Entries Aged Out - idle timeout                  8
HW Entries Aged Out - TCP FIN                       0
HW Entries Aged Out - TCP RST                       0
HW Entries Aged Out - invalid dst                   0
HW Entries Force HW Invalidate                      0
HW Entries Invalidate due to server down            0
TCAM Flows Created                                  1
TCAM Flows Freed                                    1
```

```
TCAM Flow Count                                          0
```

The following table describes the fields in the show command output.

Field	Description
HW Entries Created	Total number of hardware entries created.
HW Entry Creation Failed	Total number of times creation of hardware entries failed.
HW Entry Creation Failed - server down	Number of times creation of hardware entries failed since the server was down.
HW Entry Creation Failed - max entries exceeded	Number of times creation of hardware entries failed since the maximum entry count exceeded.
HW Entries Freed	Total number of hardware entries freed.
HW Entries Freed - opposite tuple entry aged-out	Number of hardware entries freed since the opposite tuple entry aged-out.
HW Entry Freed - no HW prog	Number of hardware entries freed since a hardware function was unavailable.
HW Entry Freed - no matched conn	Number of hardware entries freed since no connection matched.
HW Entry Freed - no software entry	Number of hardware entries freed since the software entry was not available.
HW Entries Count	Total number of hardware entries.
HW Entries Aged Out	Total number of hardware entries that aged-out.
HW Entries Aged Out - idle timeout	Number of hardware entries that aged-out due to idle timeout.
HW Entries Aged Out - TCP FIN	Number of hardware entries that aged-out after receiving a TCP FIN packet.
HW Entries Aged Out - TCP RST	Number of hardware entries that aged-out after receiving a TCP RST packet.
HW Entries Aged Out -	Number of hardware entries that aged-out

Field	Description
invalid dst	due to an invalid destination address.
HW Entries Force HW Invalidate	Number of hardware entries invalidated forcefully.
HW Entries Invalidate due to server down	Number of hardware entries invalidated since the server was down.
TCAM Flows Created	Total number of TCAM flows created.
TCAM Flows Freed	Total number of TCAM flows freed.
TCAM Flow Count	Total number of TCAM flows.

show counters cgnv6 lsn per-instance

Description Display dynamic LSN per VRID/User-Group counters. Each counter-block is differentiated by its key-name.

Syntax

```
show counters cgnv6 lsn per-instance
```

NOTE: This command does not support filters.

Example The following command displays the counters:

```
key-name = lsn-nat-44-instance-0
/cgnv6/lsn/per-instance

_____________________________________
Data Session Created 0
Data Session Freed 0
TCP Full-cone Session Created 0
TCP Full-cone Session Freed 0
UDP Full-cone Session Created 0
UDP Full-cone Session Freed 0
User-Quota Created 0
User-Quota Freed 0
TCP Ports Allocated 0
TCP Ports Freed 0
UDP Ports Allocated 0
UDP Ports Freed 0
ICMP Ports Allocated 0
```

```
ICMP Ports Freed 0

----------------------------------------
key-name = lsn-nat-64-instance-0
/cgnv6/lsn/per-instance

----------------------------------------
Data Session Created 4
Data Session Freed 4
TCP Full-cone Session Created 0
TCP Full-cone Session Freed 0
UDP Full-cone Session Created 0
UDP Full-cone Session Freed 0
User-Quota Created 4
User-Quota Freed 4
TCP Ports Allocated 0
TCP Ports Freed 0
UDP Ports Allocated 4
UDP Ports Freed 4
ICMP Ports Allocated 0
ICMP Ports Freed 0

----------------------------------------
key-name = lsn-nat-dslite-instance-0
/cgnv6/lsn/per-instance

----------------------------------------
Data Session Created 0
Data Session Freed 0
TCP Full-cone Session Created 0
TCP Full-cone Session Freed 0
UDP Full-cone Session Created 0
UDP Full-cone Session Freed 0
User-Quota Created 0
User-Quota Freed 0
TCP Ports Allocated 0
TCP Ports Freed 0
UDP Ports Allocated 0
UDP Ports Freed 0
ICMP Ports Allocated 0
ICMP Ports Freed 0
```

The following table describes the fields in this command's output.

Field	Description
Data Session Created	Total number of LSN data sessions created for that instance.
Data Session Freed	Total number of LSN data sessions freed for that instance.
TCP Full-cone Session Created	Total number of LSN TCP full-cone sessions created for that instance.
TCP Full-cone Session Freed	Total number of LSN TCP full-cone sessions freed for that instance.
UDP Full-cone Session Created	Total number of LSN UDP full-cone sessions created for that instance.
UDP Full-cone Session Freed	Total number of LSN UDP full-cone sessions freed for that instance.
User-Quota Created	Number of port mappings created for that instance, for which the user quota had available mappings.
User-Quota Freed	Number of port mappings that were created for that instance, for which the user quota had available mappings, that were later freed.
TCP Ports Allocated	Total number of TCP ports allocated for user sessions, for that instance.
TCP Ports Freed	Total number of TCP ports freed for use by other sessions, for that instance
UDP Ports Allocated	Total number of UDP ports allocated for user sessions, for that instance.
UDP Ports Freed	Total number of UDP ports freed for use by other sessions, for that instance.
ICMP Ports Allocated	Total number of ICMP ports allocated for user sessions, for that instance.

Field	Description
ICMP Ports Freed	Total number of ICMP ports freed for use by other sessions, for that instance.

show counters cgnv6 nat pool

Description Display the counters displayed in the cgnv6 NAT pool.

Syntax

```
show counters cgnv6 nat pool[
```

Example The following command displays the counters:

```
/cgnv6/nat/pool/pool1
************************************
Users
  1
ICMP
  0
ICMP Freed
  0
ICMP Total
  0
ICMP Reserved
  0
ICMP Peak
  0
ICMP Hit Full
  0
UDP
  0
UDP Freed
  0
UDP Total
  0
UDP Reserved
  64507
UDP Peak
  0
```

```
UDP Hit Full
  0
UDP Port Overloaded
  0
UDP Port Overloading Session Created
  0
UDP Port Overloading Session Freed
  0
TCP
  0
TCP Freed
  0
TCP total
  0
TCP Reserved
  64507
TCP Peak
  0
TCP Hit Full
  0
TCP Port Overloaded
  0
TCP Port Overloading Session Created
  0
TCP Port Overloading Session Freed
  0
IP Used
  1
IP Free
  0
IP Total
  1
```

The following table describes the fields in this command's output.

Field	Description
Users	Number of inside IP addresses currently using the NAT IP address.

Field	Description
ICMP/UDP/TCP/IP	Number of identifiers currently in use.
Freed	Total number of identifiers freed.
Total	Total number of identifiers allocated.
Reserved	Displays the pool IP addresses with the most total reserved ports.
Peak	Displays Peak Statistics
Hit Full	Number of times the traffic hit the port
Port Overloaded	Number of times a port on a NAT address was assigned to a new client while another client was still using the mapping. Note: This counter and the other Port Overloading counters apply only if port overloading is configured.
Port Overloaded Session Created	Number of times a session on an overloaded port was created.
Port Overloaded Session Freed	Number of times a session created on an overloaded TCP port was freed.

show counters cgnv6 nat64 hw-accelerate

Description Display hardware forwarding statistics for NAT64 sessions.

Syntax `show counters cgnv6 nat64 hw-accelerate`

Example The following command displays information related to NAT64 sessions accelerated to the hardware:

```
ACOS(config)# show counters cgnv6 nat64 hw-accelerate
show counters cgnv6 nat64 hw-accelerate
************************************
HW Entries Created                                  4
HW Entry Creation Failed                            0
HW Entry Creation Failed - server down              0
HW Entry Creation Failed - max entries exceeded     0
HW Entries Freed                                    4
```

```
HW Entries Freed - opposite tuple entry aged-out        2
HW Entry Freed - no HW prog                             0
HW Entry Freed - no matched conn                        0
HW Entry Freed - no software entry                      16
HW Entries Count                                        0
HW Entries Aged Out                                     8
HW Entries Aged Out - idle timeout                      8
HW Entries Aged Out - TCP FIN                           0
HW Entries Aged Out - TCP RST                           0
HW Entries Aged Out - invalid dst                       0
HW Entries Force HW Invalidate                          0
HW Entries Invalidate due to server down                0
TCAM Flows Created                                      2
TCAM Flows Freed                                        2
TCAM Flow Count                                         0
```

The following table describes the fields in this command's output.

Field	Description
HW Entries Created	Total number of hardware entries created.
HW Entry Creation Failed	Total number of times creation of hardware entries failed.
HW Entry Creation Failed - server down	Number of times creation of hardware entries failed since the server was down.
HW Entry Creation Failed - max entries exceeded	Number of times creation of hardware entries failed since the maximum entry count exceeded.
HW Entries Freed	Total number of hardware entries freed.
HW Entries Freed - opposite tuple entry aged-out	Number of hardware entries freed since the opposite tuple entry aged-out.
HW Entry Freed - no HW prog	Number of hardware entries freed since a hardware function was unavailable.
HW Entry Freed - no matched conn	Number of hardware entries freed since no connection matched.
HW Entry Freed - no	Number of hardware entries freed since

Field	Description
software entry	the software entry was not available.
HW Entries Count	Total number of hardware entries.
HW Entries Aged Out	Total number of hardware entries that aged-out.
HW Entries Aged Out - idle timeout	Number of hardware entries that aged-out due to idle timeout.
HW Entries Aged Out - TCP FIN	Number of hardware entries that aged-out after receiving a TCP FIN packet.
HW Entries Aged Out - TCP RST	Number of hardware entries that aged-out after receiving a TCP RST packet.
HW Entries Aged Out - invalid dst	Number of hardware entries that aged-out due to an invalid destination address.
HW Entries Force HW Invalidate	Number of hardware entries invalidated forcefully.
HW Entries Invalidate due to server down	Number of hardware entries invalidated since the server was down.
TCAM Flows Created	Total number of TCAM flows created.
TCAM Flows Freed	Total number of TCAM flows freed.
TCAM Flow Count	Total number of TCAM flows.

show ip anomaly-drop statistics

Description Display IP anomaly drop filtering statistics

Syntax

```
show ip anomaly-drop statistics
```

Mode All

Example The following command displays sample output for IP anomaly drop statistics:

```
ACOS(config)#show ip anomaly-drop statistics
IP Anomaly Drop Statistics
--------------------------
Land Attack Drop                          0
```

```
Empty Fragment Drop                         0
Micro Fragment Drop                         0
IPv4 Options Drop                           0
IP Fragment Drop                            0
Bad IP Header Len Drop                      0
Bad IP Flags Drop                           0
Bad IP TTL Drop                             0
No IP Payload drop                          0
Oversize IP Payload Drop                    0
Bad IP Payload Len Drop                     0
Bad IP Fragment Offset Drop                 0
Bad IP Checksum Drop                        0
ICMP Ping of Death Drop                     0
TCP Bad Urgent Offset Drop                  0
TCP Short Header Drop                       0
TCP Bad IP Length Drop                      0
TCP Null Flags Drop                         0
TCP Null Scan Drop                          0
TCP Syn and Fin Drop                        0
TCP XMAS Flags Drop                         0
TCP XMAS Scan Drop                          0
TCP Syn Fragment Drop                       0
TCP Fragmented Header Drop                  0
TCP Bad Checksum Drop                       0
UDP Short Header Drop                       0
UDP Bad Length Drop                         0
UDP Kerberos Fragment Drop                  0
UDP Port Loopback Drop                      0
UDP Bad Checksum Drop                       0
Runt IP Header Drop                         0
Runt TCP/UDP Header Drop                    0
IP-over-IP Tunnel Mismatch Drop             0
TCP Option Error Drop                       0
IP-over-IP Tunnel Error Drop                0
VXLAN Tunnel Error Drop                     0
GRE Tunnel Error Drop                       0
GRE PPTP Error Drop                         0
IPv6 Hop by Hop Header Drop                 0
IPv6 Destination Header Drop                0
IPv6 Routing Header Drop                    0
```

```
IPv6 Fragmentation Header Drop            0
IPv6 Authentication Header Drop           0
IPv6 ESP Header Drop                      0
IPv6 Mobility Header Drop                 0
IPv6 No Next Header Drop                  0
IPv6 Unknown Extension Header Drop        0
IPv6 Malformed Extension Header Drop      0
```

NOTE: The counter for an anomaly increments only if filtering and dropping for that anomaly type is enabled.

show/clear lsn-alg esp

Description Show counters for LSN-ALG ESP.

Syntax

```
show counters cgnv6 lsn alg esp
```

Mode All

Usage Used to view the counter values for the lsn alg esp.

Example The following command shows the counter for LSN-ALG ESP:

```
ACOS (config) #show counters cgnv6 lsn alg esp
ESP Sessions Created                                    0
nat ip conflict                                         0
```

The following table describes the fields in this output.

Parameter	Description
ESP Sessions Created	The number of esp data session created.
nap ip conflict	The number of NAT IP conflict detected.

show/clear nat64-alg esp

Description Show counters for NAT64-ALG ESP

Syntax

```
show counters cgnv6 nat64 alg esp
```

Mode All

Usage Used to view the counter values for the nat64-alg esp.

Example The following command shows the counters for NAT64-ALG ESP:

```
ACOS (config) #show counters cgnv6 nat64 alg esp
ESP Sessions Created                                          0
nat ip conflict                                          0
```

The following table describes the fields in this output:

Parameter	Description
ESP Sessions Created	The number of esp data session created.
nat ip conflict	The number of NAT IP conflict detected.

Firewall

Firewalls offer enhanced security for network PCs by preventing hackers from infecting devices with malicious software, such as viruses, worms, spy ware and other threats. A firewall enables network administrators to dictate which computers can connect to the public internet. It prevents user from accessing potentially malicious resources as well as prevent malware from accessing the internet-connected devices on your network, preventing damage to devices and theft of sensitive information.

Similarly, additional security for your web servers is provided with the Next Generation Web Application Firewall (NGWAF) feature. For more information, see Next Generation Web Application Firewall.

This reference lists the CLI configuration and show commands that apply specifically to Firewall.

Configuration Commands

fw active-rule-set

Description Activate the firewall function using the specified Access Control rule-set in an application delivery partition. The rule-set must exist prior to activating. Only one Access Control rule-set may be active in a partition.

Syntax

```
[no] fw active-rule-set rule-set-name  [session-aging template-name]
override-nat-aging
```

Parameter	Description
rule-set-name	Specify the predefined rule-set to be activated.
session-	Bind the session-aging template (for TCP, UDP, and

Parameter	Description
aging *template-name*	ICMP sessions), with the template name, to the active rule-set.
override-nat-aging	Set to override NAT aging for the active rule-set.

Default No default active rule-set.

Mode Configuration mode

Usage While ACOS supports creation of many rule-sets, only one rule-set can be active at a time.

NOTE: It may take approximately 10 seconds for the “rule-set” to become active.

Example This example shows how to activate firewall rule set *rule-set-1*:

```
ACOS(config)# fw active-rule-set rule-set-1
```

Related Commands:

- fw session-aging

fw alg

Description Configure application protocol inspection for common applications protocols, such as FTP, TFTP, SIP, DNS and others, on their well-known ports.

Syntax

```
[no] fw alg options
```

Parameter	Description
dns default-port-disable	Change DNS ALG settings for default port 53.
esp default-port-disable	Change ESP ALG settings for default port 500.

Parameter	Description
esp sampling-enable *options*	Enable sampling when certain events occur. You can specify one of the following events: • **session-created**: ESP sessions are created • **helper-created**: ESP helper sessions are created • **helper-freed**: ESP helper sessions freed • **helper-freed-used**: Used ESP helper sessions freed • **helper-freed-unused**: Unused ESP helper sessions freed • **helper-already-used**: ESP helper sessions already used • **helper-in-rml**: ESP helper session added to remove list • **all** : All events. So, enable sampling if any of the above-mentioned events occur.
ftp default-port-disable	Change FTP ALG settings for default port 21.
icmp disable	Disable ICMP ALG, which allows ICMP errors to pass through the firewall.
pptp default-port-disable	Change PPTP ALG settings for default port 1723.
rtsp default-port-disable	Change RTSP ALG settings for default port 554.
sctp { disable | enable }	Disable or enable SCTP settings.

Parameter	Description
sip default-port-disable	Change SIP ALG settings for default port 5060.
tftp default-port-disable	Change TFTP ALG settings for default port 69.

Default Application protocol inspection is enabled by default for the protocols listed in the table above. If desired, you can use this command to disable this behavior.

Mode Configuration mode

Usage ALG is enabled by default for these protocols, so traffic using common ALG protocols, (for example, FTP or SIP), may traverse the firewall without being inspected, as long as the traffic is using its associated well-known port. However, this command can be used to block traffic on the well-known ports for these protocols. To enable application protocol inspection on non-default ports, you can specify them while creating a service-rule or service object-group element.

Example The following example shows how to disable the ALG for DNS on its well-known port 53:

```
ACOS(config)# fw alg dns default-port-disable
```

fw alg-processing

Description Override the rules in a rule-set, to allow ALG traffic connections to be created, regardless of configured firewall rules that would otherwise deny the connection request.

Syntax

```
[no] fw alg-processing options
```

Parameter	Description
honor-rule-set	Honor the firewall rule-set (Default)
override-rule-set	Override the firewall rule-set

Default By default, **honor-rule-set** is enabled.

Mode Configuration mode

Usage ALG protocols, such as FTP and SIP, require the firewall to open ports to accept new connections.

By default, the firewall honors the existing rule-set, meaning the firewall will permit new ALG connection requests only if the request satisfies the explicitly configured firewall rules.

However, you can override this behavior, so that the firewall will ignore the configured firewall rules in the active rule-set. In this case, the firewall will allow the ALG connection to open the port, even if the configured rules in the rule-set would otherwise prevent the connection from opening.

Example The following example shows how to override the rules in the rule-set to allow ALG traffic to pass, regardless of whether those rules would deny the request:

```
ACOS(config)# fw alg-processing override-rule-set
```

fw allow-non-syn-session-create

Description Forward non-SYN TCP packets (except FIN and RST) by creating an established firewall session. The command supports IPv4 as well as IPv6 packets.

NOTE:

- The firewall session is created only when the first non-SYN TCP packet matches the firewall policy.
- Rule actions for CGN and IPsec are not supported.

Syntax

```
[no] fw allow-non-syn-session-create
```

Default Disabled

Mode Configuration mode

Usage The firewall drops non-SYN TCP packets since there is no session to process them. Enabling this command creates an established firewall session that processes and forwards the non-SYN TCP packets.

NOTE:

- You cannot configure this command if the **fw tcp syn-cookie** command is configured globally or the TCP SYN cookie protection is enabled in the rule of the firewall rule-set.
- Since DNS uses port 53 as a default port for transmitting DNS queries, the non-SYN TCP packets are dropped even if the **fw allow-non-syn-session-create** command is enabled. To transmit non-SYN TCP packets from port 53, you need to disable the default port by executing the **no fw alg dns default-port-disable** command.

Example The following example demonstrates the command usage:

```
ACOS(config)# fw allow-non-syn-session-create
```

fw apply-changes

Description Recompile the firewall rule-set immediately.

Syntax

```
fw apply-changes [forced]
```

Default N/A

Mode Configuration mode

Usage If you made any changes to the active rule-set, this command will push the updated rule-set to the running-config to make it take effect immediately.

Changes to the rule-set could include modifications to any element contained in the rule-set, such as a new rule, or changes to an object/ object-group contained within a rule, or changes to a a zone contained within a rule, and so on.

If changes are made and the command is not executed, then the changes will be eventually be applied after:

- an idle period of 10 seconds with no changes to the rule-set, OR

- after a maximum of 10 minutes of activity of constant changes in the rule-set
- the **forced** option can be used to force immediate recompile

This is an operational command and thus will not be stored in the running -config.

This command is partition-aware, meaning it will only apply to the partition in which it is invoked. If this command is executed within the shared partition, it will only take effect in the shared partition and will not impact the private partitions which have a firewall rule-set.

Example The following example shows how to invoke a rule-set recompile:

```
ACOS(config)# fw apply-changes
```

fw clear-session-filter

Description Enable or disable the clearing of Layer 4 session filter for the Firewall.

Syntax

```
[no] fw clear-session-filter { disable | enable }
```

Default Disabled

Mode Configuration mode

Example The following example enables this command:

```
ACOS(config)# fw clear-session-filter enable
```

fw client class-list

Description Configure a list of client IP addresses by binding to an IPv4 or IPv6 class-list. This list is used by ACOS to ensure consistent hashing of uplink and downlink traffic on Multi-PU platforms.

You need to create separate lists for IPv4 and IPv6 addresses.

NOTE: This command must be configured on Multi-PU platforms that use a DMZ interface, to ensure symmetrical distribution of uplink and downlink traffic.

Syntax

```
[no] fw client class-list { ipv4 | ipv6 } list-name
```

Replace *list-name* with the name of a predefined class-list.

Parameter	Description
ipv4	Specify this parameter to identify the class-list as an IPv4 class list.
ipv6	Specify this parameter to identify the class-list as an IPv6 class list.

Default None

Mode Configuration mode

Usage In case of Firewall, all IP addresses/subnets identifying the inside network (behind the **ip client** interface) need to be added to this list. Similarly, in case of CGNAT, all public IPs/subnets or NATted pools must be added to this list.

NOTE: In case of CGN, every NAT-pool change i.e., addition or removal of Subnet/IP address must reflect in the class-list entries to ensure consistent hashing on Multi-PU platforms.

Example In the following example, an IPv4 class-list s2 is created and then bound to the firewall client class-list.

```
ACOS(config)# class-list s2
ACOS(config-class list)# 11.1.1.4/32
ACOS(config-class list)# 11.1.1.1/32
ACOS(config-class list)# exit
ACOS(config)# fw client class-list ipv4 s2
```

fw ddos-protection action

Description Enable DDoS protection to block individual IP addresses or a subnet in case of a DDoS attack.

Syntax

```
[no] fw ddos-protection action { drop | redistribute-route
route-map-name {expiration seconds remove-wait-timer seconds
timer-multiply-max num forward }}
```

Parameter	Description
action {drop | redistribute-route *route-map-name* **{ expiration** *seconds* **| remove-wait-timer** *seconds* **| timer-multiply-max** *num* **| forward }}**	When a DDoS attack targeted toward a specific IP address is detected, one of the following actions can be configured: • **drop** - Log the event, add the victim IP to the local block list, and drop the packets sent to the IP locally. This is the default action. • **redistribute-route** - Log the event, notify the upstream router (via BGP) to reroute all packets, and stop rate-limiting. The *route-map-name* parameter specifies the route-map to be used for redirecting the packets. Configuring this option enables the Remotely Triggered Black Hole (RTBH) protection technique. Additional parameters: • **expiration** If the action configured is **drop**, this parameter specifies (in minutes) how long the IP traffic must be below the configured packets-per-second threshold before the IP is removed from the blacklist. If the action configured is **redistribute-route**, this parameter specifies the duration

Parameter	Description
	(in minutes) the blocked route must be disabled when a DDoS attack is detected. ACOS removes the blackhole route remotely when this duration expires. You can specify a value in the range 2-144000. The default is 5 minutes. • **`remove-wait-timer`** - Specify the maximum time (in seconds) to wait before removing an IP from the blacklist or black hole. You can specify a value in the range of 0 to 300. The default value is 300. • **`timer-multiply-max`** - Specify the maximum value of the timer multiplier for attacks that last long. You can specify a value in the range of 1 to 100. The default value is 6. During the remove-wait period, if ACOS detects a DDoS attack again, the black hole entry is re-initiated and the blackhole timer is extended by a duration that is twice the expiration time (for the first time). The second time, the duration is thrice the expiration time and this duration continues to increment until it reaches the maximum limit specified by this parameter. • **`forward`** - Specify this option to forward the traffic (instead of dropping it unconditionally) and continue rate-limiting. This allows subscribers to access the service even when RTBH is in effect.

Default Disabled

Mode Configuration mode

Usage DDoS protection is triggered only when the DDoS protection threshold is breached. This threshold is set by configuring the **ddos-protection-factor** in the template limit-policy for PPS limit.

Example In the following example, all packets are dropped, and the event is logged when the DDoS protection threshold limit is breached.

```
ACOS(config)# fw ddos-protection action drop
```

Example In the following example, when the DDoS protection threshold limit is breached, the RTBH action is triggered.

```
ACOS(config)# fw ddos-protection action redistribute-route mymap
```

Example The following example demonstrates the usage of the **forward** option. When the DDoS protection threshold limit is breached, the RTBH action is initiated. However, since the **forward** option is specified, the packets are forwarded (instead of being dropped), and the rate-limiting continues.

```
ACOS(config)# fw ddos-protection action redistribute-route mymap forward
```

For more information, refer to the *Firewall Configuration Guide*.

fw ddos-protection dynamic-blacklist

Description Configure the Firewall DDoS protection using dynamic blacklist sessions.

When this command is enabled, blacklist sessions are created dynamically i.e., **on the fly** to drop the traffic that matches the deny rules.

Syntax

```
[no] fw ddos-protection dynamic-blacklist [ enable | disable ]
[ inbound | outbound | both ] [timeout seconds ]
```

Parameter	Description
[enable |	Enable or disable protection against volumetric

Parameter	Description
disable]	DDoS attacks by creating dynamic blacklist sessions.
[inbound | outbound | both]	You can enable DDoS protection by specifying the traffic direction. The following options are available: • **inbound** - The inbound direction i.e., incoming traffic from the internet or other network segments. • **outbound** - The outbound direction i.e., outgoing traffic that originates inside the network. • **both** - Both, inbound and outbound traffic directions.
[timeout *num* **]**	The timeout value (in seconds) for dynamic blacklist sessions. Specify a value in the range 1 to 30 seconds. The default value is 5 seconds.

Default Disabled

Mode Configuration mode.

Usage Normally, when the platform intercepts a volumetric DDoS attack, a lot of traffic hits the deny rules, and packets are dropped based on the per-packet rule lookup. However, due to the high amount of traffic, the overhead of the per-packet rule lookup can cause CPU usage to spike. Configure this command to drop these packets more efficiently i.e., with minimum processing. When this command is enabled, blacklist sessions are created dynamically i.e., **on the fly** when a particular firewall deny rule is matched. Subsequent traffic that matches the blacklist session is dropped.

NOTE: Even if this command is enabled, blacklist session creation is triggered only when the CPU usage exceeds the pre-configured threshold limit.

Example The following example demonstrates command usage.

```
ACOS(config)# fw ddos-protection dynamic-blacklist enable
outbound timeout 20
```

fw ddos-protection logging

Description Configure event logging for Firewall DDoS protection.

Syntax

```
[no] fw ddos-protection logging [ enable { local | remote |
both } | disable ]
```

Parameter	Description
enable {local | remote | both}	Enable event logging for Firewall DDoS protection. The logs are generated by default when the firewall DDoS protection entries are added and removed. You can enable local or remote logging by specifying one of the following options: • **local** - Enable local logging only. • **remote** - Enable logging to remote servers and IPFIX collectors. • **both** - Enable local and remote logging.
disable	Disable local as well as remote logging for Firewall DDoS protection.

Default Enabled

Mode Configuration mode.

Example The following command enables remote logging for DDoS protection:

```
ACOS(config)# fw ddos-protection logging enable remote
```

fw ddos-protection sampling-enable

Description Enable sampling for FW DDoS protection entries. This feature allows you to select a subset of traffic for analysis instead of examining every

packet.

Syntax

```
[no] fw ddos-protection sampling-enable {all | ddos_entries_
too_many | ddos_entry_added | ddos_entry_removed | ddos_entry_
added_to_bgp | ddos_entry_removed_from_bgp | ddos_entry_add_
to_bgp_failure | ddos_entry_remove_from_bgp_failure | ddos_
packet_dropped}
```

This command enables sampling for specific DDoS events. Specify one of the following options:

Parameter	Description
all	Enable sample baselineing for all DDoS protection events.
ddos_entries_too_many	Enable sampling in case of too many DDOS entries.
ddos_entry_added	Enable sampling when a DDOS entry added.
ddos_entry_removed	Enable sampling when aDDOS entry is removed.
ddos_entry_added_to_bgp	Enable sampling when a DDoS entry is added to BGP.
ddos_entry_removed_from_bgp	Enable sampling when a DDoS entry is removed from BGP.
ddos_entry_add_to_bgp_failure	Enable sampling if addition of a DDoS entry to BGP fails.
ddos_entry_remove_from_bgp_failure	Enable sampling if removal of a DDoS entry from BGP fails.
ddos_packet_dropped	Enable sampling when DDOS packets are dropped.

Default Not enabled.

Mode Configuration mode

fw disable-application-category

Description Disable the application category specified.

Syntax

```
[no] fw disable-application-category application_category
```

You can specify one of the following application categories:

Application Category	Description
aaa	The protocol or application used for AAA (Authentication, Authorization and Accounting) purposes
adult-content	The protocol or application used for adult content
advertising	The protocol or application used for advertising networks
application-enforcing-tls	The application known to enforce HSTS and thus use of TLS
analytics-and-statistics	The protocol or application used for user analytics and statistics
anonymizers-and-proxies	The protocol or application used for traffic-anonymization
audio-chat	The protocol or application used for audio chat
basic	All protocols required for basic classification are included, such as most networking protocols and standard protocols like HTTP.
blog	The blogging platform protocol or application
cdn	The protocol or application used for Content-Delivery Networks
certification-authority	The protocol or application used for Certification Authority for SSL/TLS certificate
chat	The protocol or application used for text chat
classified-ads	The protocol or application used for Classified Advertisements
cloud-based-services	The protocol or application used for SaaS and/or PaaS cloud-based services

Application Category	Description
crowdfunding	The protocol or application offering service for funding a project or venture by raising small amounts of money from many people, typically via the Internet
cryptocurrency	The protocols offering services for mining crypto-currencies, for example a Crypto Web Browser (an application that mines crypto currency in the background while its user browses the web)
database	The database-specific protocols
disposable-email	The protocol or application used for the service offering Disposable Email Accounts (DEA). DEA is a technique to share temporary email address between many users
ebook-reader	The protocols offering services for e-book readers, i.e., connected devices that display electronic books
education	The protocols offering education services and online courses
email	The native email protocol
enterprise	The protocol or application used in an enterprise network
file-management	The protocol or application designed specifically for file management and exchange. This also includes bona fide network protocols (like SMB) as well as web/cloud services (like Dropbox)
file-transfer	The protocol that offers file transferring as a secondary feature. This typically includes IM, WebMail, and other protocols that allow file transfers in addition to their principal function
forum	The online forum protocol or application

Application Category	Description
gaming	The protocol or application used by games
healthcare	The protocols offering medical services, i.e protocols used in medical environment
instant-messaging-and-multimedia-conferencing	The protocol or application used for Instant Messaging or Multi-Conferencing
internet-of-things	The protocol or application used for Internet Of Things (IoT)
map-service	The protocol or application offering Digital Maps service
mobile	The mobile-specific protocol or application
multimedia-streaming	The protocol or application used for multimedia streaming
networking	The protocol used for (inter) networking purpose
news-portal	The protocol or application used for News Portals
payment-service	The application offering online services for accepting electronic payments by a variety of payment methods (credit card, bank-based payments such as direct debit, bank transfer, etc)
peer-to-peer	The protocol or application used for Peer-to-peer purposes
remote-access	The protocol or application used for remote access
scada	SCADA (Supervisory control and data acquisition) protocols
social-networks	Social networking applications
software-update	Auto-update protocols

Application Category	Description
speedtest	Speedtest application allowing to access quality of Internet connection (upload, download, latency, etc)
standards-based	The protocol issued from standardized bodies such as IETF, ITU, IEEE, ETSI, OIF
transportation	The protocols offering transportation services, for example smartphone applications that allow users to hail a taxi
video-chat	The protocol or application used for Video Chat
voip	The application used for Voice-Over-IP
vpn-tunnels	The protocol or application used for VPN or tunnelling purposes
web	The application based on HTTP/HTTPS
web-e-commerce	The protocol or application used for E-commerce websites
web-search-engines	The protocol or application used for Web search portals
web-websites	The protocol or application used for Company Websites
webmails	The application for web-based email
web-ext-adult	The application for adult web extension
web-ext-auctions	The application for auction web extension
web-ext-blogs	The application for blog web extension
web-ext-business-and-economy	The application for Business and Economy web extension
web-ext-cdns	The application for CDN web extension
web-ext-collaboration	The application for collaboration web extension

Application Category	Description
web-ext-computer-and-internet-info	The application for Computer and Internet Information web extension
web-ext-computer-and-internet-security	The application for Computer and Internet Security web extension
web-ext-dating	The application for dating web extension
web-ext-educational-institutions	The application for Educational Institution web extension
web-ext-entertainment-and-arts	The application for Entertainment and Arts web extension
web-ext-fashion-and-beauty	The application for Fashion and Beauty web extension
web-ext-file-share	The application for File Share web extension
web-ext-financial-services	The application for Financial Services web extension
web-ext-gambling	The application for gambling web extension
web-ext-games	The application for gaming web extension
web-ext-government	The application offering government web extension
web-ext-health-and-medicine	The application offering Health and Medicine web extension
web-ext-individual-stock-advice-and-tools	The application offering Individual Stock Advice and Tools web extension
web-ext-inter-	The application offering Internet Portals web

Application Category	Description
net-portals	extension
web-ext-job-search	The application for Job Search web extension
web-ext-local-information	The application offering Local Information web extension
web-ext-malware	The application offering Malware web extension
web-ext-motor-vehicles	The application for motor vehicles web extension
web-ext-music	The application offering music web extension
web-ext-news	The application offering news web extension
web-ext-p2p	The application offering P2P web extension
web-ext-parked-sites	The application offering Parked Sites web extension
web-ext-proxy-avoid-and-anonymizers	The application for Proxy Avoid and Anonymizers web extension
web-ext-real-estate	The application for real estate web extension
web-ext-reference-and-research	The application for reference and research web extension
web-ext-search-engines	The application for search engine web extension
web-ext-shopping	The application offering shopping web extension
web-ext-social-network	The application for social network web extension
web-ext-society	The application for Society web extension
web-ext-soft-	The application offering software web extension

Application Category	Description
ware	
web-ext-sports	The application for sports web extension
web-ext-streaming-media	The application offering streaming media web extension
web-ext-training-and-tools	The application offering training and tools web extension
web-ext-translation	The application offering translation web extension
web-ext-travel	The application offering travel web extension
web-ext-web-advertisements	The application offering web advertisements web extension
web-ext-web-based-email	The application offering web-based email web extension
web-ext-web-hosting	The application offering web hosting web extension
web-ext-web-service	The application offering web service web extension

Default None

Mode Configuration mode

Example The following example shows how to disable the **classified-ads** category:

```
ACOS(config)# fw disable-application-category classified-ads
```

fw disable-application-metrics

Description Disable exporting of application protocol or application category statistics to the Harmony Controller.

Syntax

```
[no] fw disable-application-metrics
```

Default Disabled

Mode Configuration mode

Example The following example demonstrates command usage:

```
ACOS(config)# fw disable-application-metrics
```

fw disable-application-protocol

Description Disable the application protocol specified.

Syntax

```
[no] fw disable-application-protocol protocol_name
```

Parameter	Description
protocol_name	Specify the application protocol name (length 1-128) that needs to be disabled.

Default None

Mode Configuration mode

Example The following example shows how to disable the **SSH** protocol:

```
ACOS(config)# fw disable-application-protocol ssh
```

fw disable-ip-fw-sessions

Description Disable auto-creation of data sessions for non-TCP/UDP/ICMP protocols that match a firewall permit rule.

Syntax

```
[no] fw disable-ip-fw-sessions
```

Default N/A

Mode Configuration mode

Usage The DC Firewall will create an associated data session for all non-TCP/UDP/ICMP protocols that match a firewall permit rule. Use this command to disable auto-creation of a separate data session.

Example The following example shows how to disable auto-creation of data sessions for non-TCP/UDP/ICMP protocols.

```
ACOS(config)# fw disable-ip-fw-sessions
```

fw disable-undetermined-rule-logs

Description Disable the logs with undetermined rules. These logs are not sent to the syslog server.

This command is available per partition.

NOTE: This command does not affect the firewall logs sent to the Harmony Controller.

Syntax

```
[no] fw disable-undetermined-rule-logs
```

Default Disabled

Mode Configuration mode

Usage When the application firewall is configured, some logs having undetermined rules are generated in the CEF log entry (cs2 field). Enable this command to reduce excessive logging and improve syslog readability.

Example The following example demonstrates command usage:

```
ACOS(config)# fw disable-undetermined-rule-logs
```

fw dsr-mode-support

Description Create a fully established session in the Direct Server Return (DSR) mode for TCP traffic. The session is created on receiving a single IPv4 or IPv6 TCP packet (except RST and FIN).

NOTE: If the **fw allow-non-syn-session-create** command is also enabled, a full session is created even on receiving a SYN TCP packet.

Syntax

```
[no] fw dsr-mode-support { ipv4 | ipv6 | all }
```

Parameter	Description
ipv4	Specify this option to create a fully established session on receiving any IPv4/TCP packet except RST and FIN.
ipv6	Specify this option to create a fully established session on receiving any IPv6/TCP packet except RST and FIN.
all	Specify this option to create a fully established session on receiving any TCP packet (IPv4 or IPv6) except RST and FIN.

Default Disabled

Mode Configuration mode

Usage When the ACOS device is deployed in Direct Server Return (DSR) mode, the standard TCP three-way handshake cannot be completed and therefore fully established sessions cannot be created. Only half-open sessions are created in the DSR mode. Configure the **fw dsr-mode-support** command in DSR mode to allow the creation of fully established sessions on receiving a single IPv4 or IPv6 TCP packet even if the standard three-way handshake is incomplete.

NOTE:

- Session creation is supported for TCP traffic only.
- ALG session creation is not supported.

Example The following command enables full session creation in DSR mode for IPv4 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv4
```

fw extended-matching disable

Description Disables firewall extended matching, which uses the zone configured on a rule as a matching criteria for permitting packets. By default,

extended matching is enabled for packets creating a session as well as packets matching an existing session.

Certain deployments utilize a routing configuration such that reverse packets (SYN-ACK) may arrive on a different interface than the one upon where ACOS sent the SYN. This configuration command allows bypassing zone check on packets matching existing sessions to handle such deployments.

Syntax `[no] fw extended-matching disable`

Default Extended matching is enabled by default

Mode Configuration mode

Example The following example disables fw extended matching.

```
ACOS(config)# fw extended-matching disable
```

fw gtp apn-prefix-list

Description Configure GTP rate limiting at the APN (Access Point Name) prefix level.

Syntax `[no] fw gtp apn-prefix-list <class-list-name> [ log-periodicity <frequency>]`

Parameters	Description
apn-prefix-list *<class-list-name>*	Bind the specified string class list to an APN prefix.
log-periodicity *<frequency>*	Enable logging when packets are dropped due to GTP rate limiting at the APN prefix level. The log periodicity can be set from 1 to 30 minutes. For example, if the periodicity is set to 2 minutes, a log is generated every 2 minutes for every message type providing the details on the Rate-Limiting Entity at the APN level.

Default None

Mode Configuration mode

Usage By configuring GTP rate-limiting policies at the APN prefix level, you can control and manage the traffic flow at a more granular level, ensuring optimal performance and resource utilization.

Example The following example demonstrates command usage. You need to create a string class list and bind it to the APN prefix.

```
ACOS(config)# class-list prefix1 string ac
ACOS(config-class list)# starts-with www gtp-rate-limit-policy
rate1
ACOS(config-class list)# starts-with www1 gtp-rate-limit-
policy rate2

ACOS(config)# fw gtp apn-prefix-list prefix1 log-periodicity 5
```

fw gtp enable

Description Enable GRPS Tunneling Protocol (GTP) globally.

Syntax

```
[no] fw gtp enable
```

Default None

Mode Configuration mode

fw gtp insertion-mode apn-prefix-list

Description Deploy the GTP Firewall in insertion mode.

Syntax

```
[no] fw gtp insertion-mode { monitor | skip-state-checks }
```

Parameters	Description
In the insertion mode, the GTP FW is inserted inline. You can configure one of the following options while deploying:	
monitor	The monitor mode allows for monitoring and evaluating the traffic without dropping or

Parameters	Description
	altering the packets. You can configure the monitor mode at the GTP firewall configuration level or the sub policy level. When configured at the GTP configuration level, it overrides the monitor mode configured at the sub-policy level.
skip-state-checks	In this mode, the GTP packets without the state information in an existing network are forwarded. This option is useful while deploying a new GTP firewall in an existing network with traffic flowing through preexisting GTP tunnels and the GTP firewall does not have the necessary state to accurately track those transactions. As a result, the packets may be dropped due to the lack of state information. To avoid such drops for existing sessions, this option can be configured to forward packets without a state while configuring the GTP firewall for new tunnels.

Default None

Mode Configuration mode

Example The following command enables the monitor mode while deploys the GTP firewall in insertion mode:

```
ACOS(config)# fw gtp insertion-mode monitor
```

fw gtp network-element-list-v4

Description Configure GTP rate limiting at the peer level (SGW/PGW) by binding an IPv4 class list with IPv4 network elements.

Syntax

```
[no] fw gtp network-element-list-v4 <class-list-name>
```

Default None

Mode Configuration mode

Usage By binding a class list with IPv4 network elements, the GTP firewall can apply the defined rate-limiting policies to GTP traffic exchanged with IPv4 addresses specified in the class list. This allows enforcement of rate limits on GTP traffic at the peer level, thereby managing network resources and preventing congestion or abuse.

Example The following example commands configure GTP rate limiting at the peer level. You need to create an IPv4 class list and bind it to the IPv4 network element.

```
ACOS(config)# class-list myv4list ipv4
ACOS(config-class list)# 10.1.1.1/32 gtp-rate-limit-policy
rate1
ACOS(config-class list)# 20.1.1.1/32 gtp-rate-limit-policy
rate2

ACOS(config)# fw gtp network-element-list-v4 myv4list
```

fw gtp network-element-list-v6

Description Configure GTP rate limiting at the peer level (SGW/PGW) by binding an IPv6 class list with IPv6 network elements.

Syntax

```
[no] fw gtp network-element-list-v6 <class-list-name>
```

Default None

Mode Configuration mode

Usage By binding a class list with IPv6 network elements, the GTP firewall can apply the defined rate-limiting policies to GTP traffic exchanged with IPv6 addresses specified in the class list. This allows enforcement of rate limits on GTP traffic at the peer level, thereby managing network resources and preventing congestion or abuse.

Example The following example commands binds an IPv6 class list with IPv6 network elements.

```
ACOS(config)# fw gtp network-element-list-v6 myv6list
```

fw gtp state-management

Description Manage the state of GTP tunnels by using GTP echo messages.

Syntax

```
[no] fw gtp state-management { echo-timeout timeout | enable-log }
```

Parameter	Description
echo-timeout *timeout*	Configure the timeout in minutes for GTP echo messages. This parameter determines how long the device waits before the GTP tunnel becomes non-responsive if no echo response is received. The echo timeout value is calculated using the following formula: `echo-timeout = echo interval + 2*T3_resp + 4*T3_resp... (N3request-1) times` where, • `echo interval` indicates the wait time before retransmitting the echo request after receiving the response. • `N3 requests` represent the number of retries for an echo request if no response is received. • `T3 response` indicates the wait time for the echo response while retransmitting the echo response. The default value for echo timeout is 120 minutes. You can specify a value in the range of 1 to 261 minutes.
enable-log	Enable logging for GTP echo messages.

Parameter	Description
	The logs prove to be useful for troubleshooting and monitoring the health of GTP tunnels.

Mode Configuration mode

Example The following example configures the echo timeout value and enables logging for GTP echo:

```
ACOS(config)# fw gtp state-management echo-timeout 200
ACOS(config)# fw gtp state-management enable-log
```

fw hairpin next-hop-follow

Description Configure IP/IPv6 subnet to lookup for the next hop of firewall hairpin traffic.

Syntax `[no] fw hairpin next-hop-follow {IPV4 network | IPV6 network}`

Default Disabled

Mode Global Configuration mode

Usage This command is used for firewall hairpin traffic between subscribers in Scaleout deployment or Multi-PU platform. Specifying the next-hop to the specified external router ensures that the router redirects the traffic back to the appropriate Scaleout node or Multi-PU platform and achieves traffic continuity.

NOTE: You can configure only one IPV4 network and one IPV6 network. However, for each of the networks, multiple routes can be configured. The command must be configured along with the appropriate firewall rules for hairpin traffic flow. It can be configured in the following deployments:
a. CGN to FW
b. FW to CGN
c. FW to FW

For more information on configuration details, see Scaleout Configuration Guide.

Example The following example configures the IPV4 network as the next hop to be followed for firewall hairpin traffic:

```
ACOS(config)# fw hairpin next-hop-follow 40.10.1.0 /24
ACOS (config)# ip route 40.10.1.0 /24 50.13.0.50
ACOS (config)# ip route 40.10.1.0 /24 50.13.0.51
```

Example The following example configures the IPV6 network as the next hop to be followed for firewall hairpin traffic:

```
ACOS(config)# fw hairpin next-hop-follow 5001::/16
ACOS (config)# ipv6 route 5001::/16 4001::1
```

Example The following example configures CGN to FW hairpin configuration in which the CGN and FW clients can access each other via EIF full-cone sessions and ALGs:

```
ACOS(config)# fw hairpin next-hop-follow 40.40.40.0 /24
ACOS (config)# ip route 40.10.1.0 /24 50.13.0.50
ACOS (config)# ip route 40.10.1.0 /24 50.13.0.51

ACOS(config)#rule-set rs1
ACOS(config-rule set:rs1)#rule cgn_zone
ACOS(config-rule set:rs1-rule:cgn_zone)#action permit cgnv6
lsn-lid 1
ACOS(config-rule set:rs1-rule:cgn_zone)#source ipv4-address
10.1.1.0/24
ACOS(config-rule set:rs1-rule:cgn_zone)#source zone cgn1
ACOS(config-rule set:rs1-rule:cgn_zone)#dest ipv4-address any
```

```
ACOS(config-rule set:rs1-rule:cgn_zone)#dest zone any
ACOS(config-rule set:rs1-rule:cgn_zone)#service any
ACOS(config-rule set:rs1-rule:cgn_zone)#exit
ACOS(config-rule set:rs1)#exit
ACOS(config-rule set:rs1)#rule fw_zone
ACOS(config-rule set:rs1-rule:fw_zone)#action permit listen-
on-port
ACOS(config-rule set:rs1-rule:fw_zone)#source ipv4-address
20.1.1.0/24
ACOS(config-rule set:rs1-rule:fw_zone)#source zone fw1
ACOS(config-rule set:rs1-rule:fw_zone)#dest ipv4-address any
ACOS(config-rule set:rs1-rule:fw_zone)#dest zone any
ACOS(config-rule set:rs1-rule:fw_zone)#service any
```

fw helper-sessions

NOTE: This is an internal command and should only be used by A10 Networks Technical Support for debugging purposes.

Description Configure firewall helper-sessions options (TAC use only).

Syntax `[no] fw helper-sessions {idle-timeout | limit | mode disable}`

Parameter	Description
idle-timeout	Set the firewall helper-sessions idle-timeout to a value ranging from 1-255 minutes. Default is 1 minute.
limit	Limit the number of helper sessions that can be created (1-134217728).
mode disable	Helper sessions mode is enabled by default. You can use **mode disable** to disable the creation of any helper-sessions. Use the “no” form of the command to re-enable the feature.

Mode Configuration mode

Usage Data Center Firewall can employ short-lived helper sessions to provide faster rule lookups. This can be helpful in cases where traffic is repeatedly sent to the same destination IP address and port from the same source IP address. Use the **idle-timeout** and **limit** options to change the behavior of these helper-sessions.

Example The following example sets the idle-timeout for firewall helper-sessions to 10 minutes:

```
ACOS(config)# fw helper-sessions idle-timeout 10
```

fw inbound-refresh

Description Enable or disable the session aging time for firewall data sessions.

Syntax

```
fw inbound-refresh {disable | enable}
```

Default Enabled

Mode Configuration mode

Usage This command disables or enables resetting of the age-out time for firewall data sessions when inbound packets are received. However, this command does not apply to outbound packets.

fw inbound-refresh-full-cone

Description Enable or disable the session aging time for firewall full-cone sessions.

Syntax

```
fw inbound-refresh-full-cone {disable | enable}
```

Default Enabled

Mode Configuration mode

Usage When this command is disabled, inbound packets that match an existing firewall data session are allowed. However, if the packets match a firewall full-cone session, new session will be created by the active full-cone session but rejected by the inactive full cone session and session's age will not be refreshed.

fw listen-on-port-timeout

Description Configure session's Session Traversal Utilities for NAT (STUN) timeout.

Syntax

```
[no] fw listen-on-port-timeout num
```

Default 2 minutes

Mode Configuration mode

Example The following example sets the idle-timeout for firewall helper-sessions to 60 minutes:

```
ACOS(config)# fw listen-on-port-timeout 60
```

fw local logging

Description For Application aware firewall, enables the local-log.

Syntax

```
fw local logging
```

Parameter	Description
local-log	The name of the feature. For example, app_fw - application firewall.

Default Disabled

Mode Global configuration mode

Example

```
ACOS(config)# fw local-logging
```

fw logging

Description Bind a firewall logging template to the firewall.

Syntax

```
fw logging  [ cef-label { enable | disable } | gtp [sampling-enable ] | template-name | sampling-enable ]
```

Parameter	Description
cef-label { enable | disable }	Configure this option to enable or disable the inclusion of CEF labels in the Syslog. • **enable** - Configure this option to include all CEF labels in the Syslog. This option is enabled by default. • **disable** - Configure this option to suppress all CEF labels in the Syslog. This option helps optimize log management processes, reduce logging costs, and improve the readability of logs.
gtp [sampling-enable]	Configure this option to include GTP counters in the logs.
template-name	Specify the logging template name to be bound to the firewall.
sampling-enable	Enable baselining.

Default No default logging template.

Mode Configuration mode

Usage The data center firewall creates a high volume of log messages for data events, such as when a firewall session is created or destroyed. These log messages are directed to an external logging server.

Use this **fw logging** command to bind a fw template logging to an active rule-set, or for general information about configuring an external logging host.

Configuration events also generate log messages, but these are typically sent to a different log server than the firewall data log messages. You can set up where to send the config-change logs using the standard **logging host** command.

Example The following example binds the logging template *temp-log1* to the firewall:

```
ACOS(config)# fw logging temp-log1
ACOS(config)# fw logging appfw
```

Example The following command suppresses all CEF labels in the Syslog:

```
ACOS(config)# fw logging cef-label disable
```

Related Commands:

- logging host

fw natip-ddos-protection

Description Enable or disable protection against NAT IP DDoS attacks.

NAT IP DDoS attacks exploit Network Address Translation (NAT) devices by overwhelming them with high-volume traffic, leading to service disruption.

Syntax

```
fw natip-ddos-protection {disable | enable}
```

Default Disabled

Mode Configuration mode

fw permit-default-action

Description This command applies to Gi/SGi-FW partition only. For a rule that does not have an application associated with it, this command changes the way ACOS processes incoming traffic when a match occurs on a policy rule containing “action permit”.

Syntax

```
[no] fw permit-default-action {forward | next-service-mode}
```

Parameter	Description
forward	The packet will be L3 forwarded and a firewall session will be created.

Parameter	Description
next-service-mode	The packet will be processed according to the applications configured in order.

Default By default, a “permit” rule with no application specified is L3 forwarded and will create a firewall session.

NOTE: If neither of the **forward** nor **next-service-mode** option is configured, then a firewall session will be created. Alternatively, if the **forward** option is configured, then a firewall session will be created. Lastly, if the **next-service-mode** option is configured, then a CGN session will be created.

Mode Configuration mode

Usage This command only applies to Gi/SGi-FW partitions.

A rule-set containing firewall rules control what traffic is allowed to enter on the firewall. Each rule can be configured with the “permit” action associated with a selected application to be applied to packets matching the rule. The rule can be configured as generically as “forward” or “cgnv6”, or exclusively as “cgnv6 lsn-lid 2” or “cgnv6 fixed-nat”.

Example The following example shows how to configure ACOS such that the packet will be forwarded at Layer 3 and will open a firewall session:

```
ACOS(config)# fw permit-default-action forward
```

fw respond-to-user-mac

Description Configure ACOS to use the user’s source MAC for the next hop rather than the routing table.

Syntax

```
[no] fw respond-to-user-mac
```

Default Disable

fw server

Description Configure a firewall logging server.

Syntax `[no] fw server server-name [IPv6-addr | IPv4-addr | hostname]`

Replace server-name with the name of the logging server, 1-127 characters.

Specify the IPv4 or IPv6 address, or hostname for the logging server.

This command changes the CLI to the configuration level for the specified server, where the following commands are available:

Parameter	Description
`[no] health-check [monitor-name]`	Enables health monitoring of the server. The *monitor-name* specifies the name of a configured health monitor. If you omit this command or you enter it without the monitor-name option, the default Layer 3 (ICMP) health monitor is used.
`[no] health-check-disable`	Disables health monitoring of the server.
`[no] port port-num {tcp | udp}`	Specifies the TCP or UDP port on which the server listens for traffic. **enable | disable** Enables or disables the port. **[no] health-check [*monitor-name*]** Enables health monitoring of the port. The monitor-name option specifies the name of a configured health monitor. If you omit the `health-check` command or you enter

Parameter	Description
	it without the *monitor-name* option, the default UDP health monitor is used. **[no] health-check-disable** Disables health monitoring of the port. **[no] sampling-enable** *type* Enables the baselining on the port.
[**no**]**enable** | **disable**	Enables or disables the server.

Default There are no logging servers configured by default.

Mode Configuration mode

Usage This command creates a new real server. The CLI changes to the configuration level for the server. The “no” form of this command removes an existing real server. The IP address of the server can be in either IPv4 or IPv6 format, or hostname.

Example The following example shows how to configure a logging server called “log-serv1” at 1.2.3.4:

```
ACOS(config)# fw server log-serv1 1.2.3.4
ACOS(config-real server)#
```

fw service-group

Description Configure a service group for the firewall logging server.

Syntax

```
[no] fw service-group group-name {tcp | udp}
```

Replace *group-name* with the name of the group, 1-127 characters.

Specify the application type for the service group (**tcp** or **udp**).

This command changes the CLI to the configuration level for the specified service group, where the following commands are available:

Parameter	Description
[**no**] **health-check** [*monitor-name*]	Enables health monitoring of the service group. The *monitor-name* specifies the name of a configured health monitor.
[**no**] **member** *server-name portnum* [**sampling-enable** *type*]	Adds the external log server and port to the service group. The **sampling-enable** option enables baselining on the service group member.

Default There are no service-groups configured by default.

Mode Configuration mode

Usage This command creates a new service group. The CLI changes to the configuration level for the service group.

Example The following example adds TCP service-group called “sg1”:

```
ACOS(config)# fw service-group sg1 tcp
ACOS(config-fw svc group)#
```

fw session-aging

Description Configure the session-aging template for ICMP, TCP, and UDP protocols.

Syntax

```
[no] fw session-aging  template_name
```

This command changes the CLI to the configuration level for the designated session-aging template, where the following commands are available.

Command	Description
[**no**] **icmp**	Configure idle-timeout for ICMP sessions. You can set

Command	Description
idle-timeout *seconds*	the timeout to a value ranging from 2-15000 seconds. The default is 2 seconds.
[**no**] **ip-others ip-idle-timeout** *seconds*	Configure idle-timeout for sessions that are not TCP, UDP, or ICMP traffic. You can set the timeout to a value ranging from 1-2097151 seconds. The default is 30 seconds.
[**no**] **tcp**	Configure the following options for TCP sessions: • **force-delete-timeout** *num* – Specifies the maximum time (in seconds) that a session can remain in the system before being deleted. This option forces the deletion of any session that remains active beyond the specified number of seconds. The timeout can be 1-31 seconds. The default for this option is off. • **force-delete-timeout-100ms** *num* – The maximum time that a session can remain in the system before being deleted. The timeout value is set in 100 millisecond units. You can assign a value ranging from 1-31 (multiplied by the number of 100-ms units). This option is not set by default. • **half-close-idle-timeout** *num* – Enables aging of half-closed TCP sessions. A half-closed TCP session exists when the server sends a FIN but the client does not reply with an ACK. You can set the timeout in the range of 1-120 seconds. This option is not set by default. • **half-open-idle-timeout** *num* – Enables aging of half-open TCP sessions. A half-open TCP session is one in which the client receives a SYN-ACK, but does not reply with an ACK. You can set the timeout value in the range of 1-60 seconds. This

Command	Description
	option is not set by default. • **idle-timeout** *num* – Specifies the number of seconds a connection can remain idle before the ACOS device terminates it. You can specify 1-2097151 seconds (about 24 days). If you specify 31 seconds or higher, ACOS rounds up to the next multiple of 60 seconds. The default is 600 seconds. • **port** *num* – Enables configuration of port-based timeouts for TCP ports. You can set the port number to a value from 1-65535. At this configuration point, the following sub-options are available: ◦ **force-delete-timeout** ◦ **force-delete-timeout-100ms** ◦ **half-close-idle-timeout** ◦ **half-open-idle-timeout** ◦ **idle-timeout**
[**no**] **udp**	Configure the following options for UDP sessions: • **idle-timeout** *num* – Configure the idle-timeout (seconds) for UDP sessions. You can set the timeout value in the range of 1-2097151 seconds. The default is 120 seconds. • **port** *num*– Enables configuration of port-based timeouts for UDP ports. You can set the port number to a value from 1-65535. At this configuration point, the following sub-options are available: ◦ **idle-timeout**

Mode Configuration mode

Usage Configure the session-aging template for TCP, UDP, and ICMP protocols.

Preference for idle-timeouts when multiple types have been configured:

You can configure multiple different types of timeouts, such as protocol-based and port-based idle-timeouts. There could also be an idle-timeout configured under a rule in a rule-set. In such cases where a conflict may occur, ACOS will select the idle-timeout values in the following order of precedence:

1) Idle timeouts configured at the rule level will be used first.

2) ACOS will use the port-based idle-timeout (configured within the session-aging template) if there is no rule level idle-timeout value configured.

3) ACOS will use the protocol-based idle-timeout value from the firewall session-aging template if there is no rule-level timeout and no port-based idle-timeout.

4) ACOS will use the system default idle-timeout value when there is no timeout configured at the rule level, nor at the port or protocol level within the firewall session-aging template.

NOTE: All ALG data sessions will inherit the idle-timeout values from the control session, even if the port being used has an idle-timeout value configured in the firewall session-aging template.

Example The following example shows how to configure a session-aging template *name1*. The example sets the idle-timeout for ICMP to 15 seconds:

```
ACOS(config)# fw session-aging name1
ACOS(config-session-aging:name1)# icmp idle-timeout 15
```

Example The following example sets the global TCP half-close idle timeout to 10 seconds and configures it to 5 seconds for port 1337:

```
ACOS(config)# fw session-aging name1
ACOS(config-session-aging:name1)# tcp half-close-idle-timeout
10
ACOS(config-session-aging:name1)# tcp port 1337 half-close-
idle-timeout 5
```

fw tcp mss-clamp

Description Configure the MSS Clamping values for a Gi firewall.

Syntax

```
[no] fw tcp mss-clamp { fixed fixed_value | subtract subtract_value [ min min_value ] }
```

Parameter	Description
fixed	Maximum value of the MSS-Clamping in bytes. The number ranges from 0 through 1460.
subtract	Value to subtract from the maximum MSS-Clamping value. The number ranges from 0 through 1460.
min	Minimum value of the MSS-Clamping in bytes. The number ranges from 0 through 1460. The default is 576-60-60.

Default By default, **fw tcp mss-clamp** is disabled.

Mode Configuration mode

Usage The TCP MSS value is the maximum amount of data that a network host can accept in a single TCP segment. Use the ACOS CLI to set the maximum and minimum TCP MSS values, as well as the value to subtract from the configured maximum MSS value, if the configured MSS value exceeds the MTU of the network. The MTU of the network is calculated as follows: `MTU of the network = MSS + Size of TCP-IP Headers`

Example The following example shows how to configure the maximum, subtraction, and minimum values for MSS Clamping:

```
ACOS(config)# fw tcp mss-clamp fixed 1200
ACOS(config)# fw tcp mss-clamp subtract 100 min 480
```

fw tcp reset-on-error

Description Configure the firewall to send TCP resets on error for Gi firewall.

Syntax

```
[no] fw tcp reset-on-error enable
```

Default Disabled

Mode Configuration mode

Usage If **fw tcp reset-on-error enable** is configured and the first TCP packet for a flow is not a SYN, then the firewall will send the TCP reset for "fw transparent sessions," including both IPv4 and IPv6.

Example The following example shows how to enable this feature:

```
ACOS(config)# fw tcp reset-on-error enable
```

fw tcp-rst-close-immediate

Description Configure this command to determine how fast a TCP session closes after receiving a TCP Reset (RST) packet.

Syntax

```
fw tcp-rst-close-immediate {disable | enable}
```

Parameter	Description
enable	After receiving a TCP RST packet, the Firewall immediately unlinks the TCP session from the active session table before adding it to the delete queue. Since the subsequent packets do not match the session, the TCP session closes instantly, and no packets are forwarded. This option is enabled by default.
disable	After receiving a TCP RST packet, the Firewall waits for a stipulated time (1 to 2 seconds) to unlink the TCP session from the active session table before adding it to the delete queue. If ACOS receives a packet that matches the TCP session within this time frame, the packet is forwarded.

Default Enabled

Mode Configuration mode

Usage This command enables or disables the immediate closure of a TCP session after receiving a TCP RST packet. Enabling this command (default) provides protection against TCP Reset attacks.

fw tcp syn-cookie

Description Configures SYN cookie for the firewall.

Syntax

```
[no] fw tcp syn-cookie enable [tcp-half-open on-threshold on-limit [on-timeout timeout-value]]
```

Default None.

Mode Configuration mode

Usage This command configures TCP SYN cookie which is triggered by tcp-half-open connections and disables after the timeout value.

NOTE:

- This command cannot be configured when **`fw allow-non-syn-forward`** command is enabled.
- TCP syn-cookie protection can also be enabled per firewall rule using the rule-set rule action permit command.

Example The following example configures TCP SYN cookie:

```
fw tcp syn-cookie enable tcp-half-open on-threshold 1000 on-timeout 120
```

fw tcp-window-check

Description Enable or disable firewall TCP window check.

Syntax

```
[no] fw tcp-window-check {enable | disable | sampling-enable}
```

Parameter	Description
`enable`	This option enables the TCP window check function, meaning packets outside the advertised window will be dropped. (default)

Parameter	Description
disable	This option disables the TCP window check function.
sampling-enable {all | outside-window}	This option enables baselining and rate calculation for counters. Specify one of these options: • **all** – Applies to all packets • **outside-window** – Counter for packets that were dropped for being outside the TCP window

Mode Configuration mode

Usage TCP window checks enforce that TCP packets are within the advertised window (for traffic in both directions) by tracking the sequence and acknowledgment numbers. Packets outside the advertised window are dropped.

Example The following example shows how to enable the tcp-window-check option with baselining and rate calculation enabled for packets that were outside of the advertised TCP window:

```
ACOS(config)# fw tcp-window-check enable
ACOS(config)# fw tcp-window-check sampling-enable outside-window
```

Related Commands:

- sampling-enable

fw template logging

Description Configure a firewall logging template.

Syntax

```
[no] fw template logging temp-name
```

Replace *temp-name* with the name of the logging template, 1-63 characters. This command changes the CLI to the configuration level for the specified logging template, where the following commands are available:

Parameter	Description
[no] custom message {session-created | session-deleted} *message_string*	Set custom message string by configuring the following parameters: • **session-created** - Specify this parameter to log session creation events. • **session-deleted** - Specify this parameter to log session deletion events. • *message_string* - Specify an arbitrary log message string (1-255 characters) for custom logging by including only relevant events and fields. You can also include event-specific details such as session start time, session duration, and more by using certain predefined keywords. These keywords must be enclosed in dollar signs ($). For the keyword list, see Custom Format Keywords. **NOTE:** The format custom command must be configured before setting the custom message, else firewall logs will be generated in the default CEF format.
[no] disable-log-by-destination	Disables logging by specific protocol and destination port, and range of ports. The following options are available: • **icmp** – disables logging for ICMP traffic • **ip** – configures a filter for IP entry • **ip6** – configures a filter for IPv6 entry • **others** – disables logging for other protocols • **tcp** – disables logging by destination TCP port • **udp** – disables logging by destination UDP port

Parameter	Description
[no] **enable-log-by-destination**	Enables logging by specific protocol, destination IP address, port, and range of ports. The following options are available: • **icmp** – enables logging for ICMP traffic • **ip** – configures a filter for IP entry • **ip6** – configures a filter for IPv6 entry • **others** – enables logging for other protocols • **tcp** – enables logging by destination TCP port • **udp** – enables logging by destination UDP port
[no] **facility** *options*	For the FW logging facility, specify one of the following *options*: • kernel (0: Kernel) • user (1: User-level • mail (2: Mail) • daemon (3: System daemons) • security-authorization (4: Sec/authorization) • syslog (5: Syslog internal) • line-printer (6: Line printer) • news (7: Network news) • uucp (8: UUCP subsystem) • cron (9: Time-related) • security-authorization-private (10: Private security/authorization) • ftp (11: FTP) • ntp (12: NTP) • audit (13: Audit)

Parameter	Description
	• `alert` (14: Alert) • `clock` (15: Clock-related) • `local0` (16: Local use 0) (default) • `local1` (17: Local use 1) • `local2` (18: Local use 2) • `local3` (19: Local use 3) • `local4` (20: Local use 4) • `local5` (21: Local use 5) • `local6` (22: Local use 6) • `local7` (23: Local use 7)
`[no] format {ascii | cef | custom}`	Specify the firewall logging format: • **`ascii`** – A10 Text logging format (ASCII), used to support advanced CGN logging options, such as `include-radius` and `include-http`. • **`cef`** – Common Event Format for logging (default) • **`custom`** – Custom format for logging. This parameter must be configured to enable custom logging. Configure the arbitrary log message using the custom message command.
`[no] include-dest-fqdn`	Include the destination's Fully Qualified Domain Name (FQDN) string in the logs.
`[no] include-http` *options*	Include one or more of the following HTTP fields in http-request logs: • cookie – Log HTTP Cookie Header • file-extension – HTTP file extension

Parameter	Description
	• l4-session-info – Log the L4 session information of the HTTP request • method – Log the HTTP Request Method • referer – Log HTTP Referer Header • request-number – HTTP Request Number • user-agent – Log HTTP User-Agent Header • header1 – Log HTTP Header 1 • header2 – Log HTTP Header 2 • header3 – Log HTTP Header 3
[no] **include-radius-attribute** *options*	Include one or more of the following RADIUS attributes in logs: • framed-ipv6-prefix – Include radius attributes for the prefix • imei – Include IMEI • imsi – Include IMSI • insert-if-not-existing zero-in-custom-attr – Insert 0000 for standard and custom attributes in log string • msisdn – Include MSISDN • custom1 – Customized attribute 1 • custom2 – Customized attribute 2 • custom3 – Customized attribute 3 • no-quote – No quotation marks for RADIUS attributes in logs
[no] **include-year**	Include the 4-digit year in the logs.
[no] **log http-requests** {**host**	For client HTTP requests , you can enable logging for one of the following types of information:

Parameter	Description
| **url**}	• **host** – Host requested by the client • **url** – URL requested by the client
[**no**] **resolution** {**seconds** | **10-milliseconds**}	Specifies the precision of the timestamps in log messages. • Seconds – Log message timestamps are precise to within one whole second. (default) • 10-milliseconds – Log message timestamps are precise to within 1/100 second (10 milliseconds).
[**no**] **rule http-requests** *options*	The additional rules for FW logging events. Specify one of the following *options*: • **dest-port** – Log only HTTP requests sent to specified dest port (Default: none) • **disable-sequence-check** – Disable http packet sequence check and do not drop out of order packets • **include-all-headers** – Include all configured headers despite absence in HTTP request • **log-every-http-request** – Log every HTTP request in an HTTP 1.1 session (Default: Log the first HTTP request in a session) • **max-url-len** – Max length of URL log
[**no**] **service-group** *group-name*	This option binds a service group to the logging template. *group-name* is the name of the service group. (1-127 characters)
[**no**] **severity** *options*	The minimum severity level for which log messages will be sent. Specify one of the following *options*: • 0 (emergency) • 1 (alert)

Parameter	Description
	• 2 (critical) • 3 (error) • 4 (warning) • 5 (notification) • 6 (information) • 7 (debugging) (default)
[**no**] **source-address** {**ipv** *ipv4-add* | **ipv6** *ipv6-add*}	Specify the source address of logging packet.
[**no**] **session-periodic-log interval** *number*	Specify the interval for periodic session log in minutes (1–60). The interval indicates how frequently you want to store session logs.

Default There are no logging templates configured by default.

Mode Configuration mode

Usage The custom format allows you to include event-specific details such as session start time, session duration, and more by specifying certain predefined keywords. A maximum of only 20 attributes can be configured at a time. The following tables list the keywords that can be included in the custom logging format:

Keywords for **session-creation** event:

Keyword	Description	Example Output in logs
$proto-name$	Protocol used in the session.	UDP/TCP

Keyword	Description	Example Output in logs
$src-ip$	Source IP address of the session.	5.5.5.100
$src-port$	Source Port number of the session.	34273
$dst-ip$	Destination IP address of the session.	6.6.6.100
$dst-port$	Destination Port number of the session.	2123
$in-interface$	Incoming network interface of the session.	ve801
$out-interface$	Outgoing network interface of the session.	ve701
$rule-set-name$	Specific rule set applied to the session.	rule-set1
$rule-name$	Specific rule name within the rule set that matched the session.	rule1
$partition-name$	Partition within the Firewall where the session exists.	p1
$sesn-start-time$	Start time of the session.	20190520062105
$sesn-start-time-epoch$	Epoch start time of the session.	1726081258
$time-stamp$	Log generation time stamp	20200510062005
$src-zone$	Source Zone	outside
$dest-zone$	Destination Zone	inside
$app-id$	App Id	5
$radius-msisdn$	RADIUS attribute: MSISDN	999

Keyword	Description	Example Output in logs
`$radius-imei$`	RADIUS attribute: IMEI	999
`$radius-imsi$`	RADIUS attribute: IMSI	999
`$radius-ctm1`	RADIUS attribute: Custom1	a222
`$radius-ctm2$`	RADIUS attribute: Custom2	b222
`$radius-ctm3$`	RADIUS attribute: Custom3	c222
`$radius-ctm4`	RADIUS attribute: Custom4	d222
`$radius-ctm5`	RADIUS attribute: Custom5	e222
`$radius-ctm6`	RADIUS attribute: Custom6	f222

Keywords for `session-delete` event:

Keyword	Description	Example Output in logs
`$proto-name$`	Protocol used in the session.	UDP/TCP
`$src-ip$`	Source IP address of the session.	5.5.5.100
`$src-port$`	Source Port number of the session.	34273
`$dst-ip$`	Destination IP address of the session.	6.6.6.100
`$dst-port$`	Destination Port number of the session.	2123
`$in-inter-`	Incoming network interface of the	ve801

Keyword	Description	Example Out-put in logs
face$	session.	
$out-inter-face$	Outgoing network interface of the session.	ve701
$rule-set-name$	Specific rule set applied to the session.	rule-set1
$rule-name$	Specific rule name within the rule set that matched the session.	rule1
$partition-name$	Partition within the Firewall where the session exists.	p1
$sesn-start-time$	Start time of the session.	20190520062105
$sesn-start-time-epoch$	Epoch start time of the session.	1726081258
$sesn-dur$	Total time the session was active.	12
$in-bytes$	Total number of bytes received during the session.	0
$out-bytes$	Total number of bytes sent during the session.	187
$pkts-rx$	Total number of packets received by the session.	0
$pkts-tx$	Total number of packets transmitted (sent) from the session.	1
$sesn-end-time$	Session end time	20190520062200
$sesn-end-time-epoch$	Epoch end time of the session.	1726081272
$time-stamp$	Log generation time stamp	20200510062005

Keyword	Description	Example Out-put in logs
$src-zone$	Source Zone	outside
$dest-zone$	Destination Zone	inside
$app-id$	App Id	5
$radius-msisdn$	RADIUS attribute: MSISDN	999
$radius-imei$	RADIUS attribute: IMEI	999
$radius-imsi$	RADIUS attribute: IMSI	999
$radius-ctm1	RADIUS attribute: Custom1	a222
$radius-ctm2$	RADIUS attribute: Custom2	b222
$radius-ctm3$	RADIUS attribute: Custom3	c222
$radius-ctm4	RADIUS attribute: Custom4	d222
$radius-ctm5	RADIUS attribute: Custom5	e222
$radius-ctm6	RADIUS attribute: Custom6	f222

NOTE: In case of traffic routed through CGN and Firewall, it is recommended to use the NAT logging template instead of the Firewall logging template.

Example The following example shows how to configure a firewall logging template called “n1” with service-group “sg1”:

```
ACOS(config)# fw template logging n1
ACOS(config-logging)# service-group sg1
ACOS(config-logging)# session-periodic-log interval 2
```

Example The following example shows how to enable the custom logging format and configure the custom message:

```
ACOS(config)# fw template logging custom_template
ACOS(config-logging)# format custom
ACOS(config-logging)# custom message session-created FW_
SESSION_CREATED,$src-ip$,$src-port$,$proto-name$,$dst-
ip$,$dst-port$,$sesn-start-time$,$rule-set-name$,$rule-
name$,$in-interface$,$sesn-start-time-epoch$,$time-
stamp$,$src-zone$,$dest-zone$,$app-id$,$radius-
msisdn$,$radius-ctm1$,$radius-ctm2$
ACOS(config-logging)# custom message session-deleted FW_
SESSION_DELETED,$src-ip$,$src-port$,$proto-name$,$dst-
ip$,$dst-port$,$sesn-start-time$,$sesn-dur$,$rule-set-
name$,$rule-name$,$pkts-rx$,$sesn-start-time-epoch$,$sesn-end-
time$,$sesn-end-time-epoch$,$time-stamp$,$src-zone$,$app-
id$,$radius-msisdn$,$radius-ctm1$
```

Corresponding logs generated in custom format:

```
FW_SESSION_
CREATED,10.0.0.6,1769,UDP,20.0.0.4,0,20240425223523,rs1,rule1,
ve2,1726081258,outside,
inside, 5,999,a222,b222
FW_SESSION_
DELETED,10.0.0.6,1768,UDP,20.0.0.4,0,20240425223543,14559,rs1,
rule1,0,1726081258,
20190520062200,1726081272,inside,5,999,a222
```

Example The following commands enable the TCP port and UDP port for logging:

```
ACOS(config)# fw template logging temp
ACOS(config-logging)# enable-log-by-destination
ACOS(config-logging-filter)# tcp port 9000
ACOS(config-logging-filter)# udp port 657
```

Example The following commands enable the IPv4 address for logging:

```
ACOS(config)# fw template logging temp
ACOS(config-logging)# enable-log-by-destination
ACOS(config-logging-filter)# ip 20.1.0.1/32
ACOS(config-logging-filter-ip)# udp port 5679
```

```
ACOS(config-logging-filter-ip)# tcp port 90
```

Example The following commands disable the TCP port and UDP port for logging:

```
ACOS(config)# fw template logging temp
ACOS(config-logging)# disable-log-by-destination
ACOS(config-logging-filter)# tcp port 7000
ACOS(config-logging-filter)# udp port 564
```

Example The following commands disable the IPv4 address for logging:

```
ACOS(config)# fw template logging temp
ACOS(config-logging)# disable-log-by-destination
ACOS(config-logging-filter)# ip 20.1.0.1/32
ACOS(config-logging-filter-ip)# tcp port 7000
ACOS(config-logging-filter-ip)# udp port 564
```

fw urpf

Description Configure the Unicast Reverse Path Forwarding (URPF) technique to help validate the source IP address of the incoming packets.

Syntax

```
[no] fw urpf { loose | strict | disable }
```

Parameter	Description
strict	Configure the URPF technique in strict mode. The strict mode ensures that the source IP address of the incoming packet has a route in the routing table and the route points back to the same interface through which the packet arrived.
loose	Configure the URPF technique in loose mode. This option is enabled by default. The loose mode only confirms the presence of any route to the source IP address in the routing table, irrespective of the interface. This mode is less effective at preventing IP spoofing as

Parameter	Description
	compared to the strict mode.
disable	Disable the URPF technique.

Default **loose**

Mode Configuration mode

Usage When this command is configured, ACOS creates a session only if the reverse route to the IPv4 or IPv6 source address follows the same interface through which the packet was received. This ensures that the packet follows a legitimate path, and thus helps prevent IP address spoofing.

Example The following command enables URPF in strict mode :

```
ACOS(config)# fw urpf strict
```

fw vrid

Description Configure a VRID group number for VRRP-A redundancy.

Syntax

```
[no] fw vrid vrid-group
```

Parameter	Description
[no] vrid *vrid-group*	Allow this ACOS device to join a VRRP-A group id. *vrid-group* The *vrid-group* can be a number ranging from 1-31.

Default No default

Mode Configuration mode

Usage For more information, see Configuring VRRP-A High Availability for adding the firewall to a group of ACOS devices set up for VRRP-A redundancy.

Example The following example shows how to add this firewall to vrid-group 3:

```
ACOS(config)# fw vrid 3
ACOS(config)#
```

object-group application

Description For Application aware firewall, configures the object group for an application.

Syntax

```
object-group application object name
```

Parameter	Description
category	Specify application category
clear	Clear or reset functions
do	Run executional commands in configuration mode
end	Exit from the configuration mode
exit	Exit from the configuration mode or the sub mode
no	Negate a command or set its defaults
protocol	Specify one or more applications
show	Display running system configuration
user-tag	Display customized tag
write	Write or save the configuration

Default Disabled

Mode Global configuration mode

Example

```
ACOS (config)#object-group application app-obj-grp-1 protocol
dns
```

rule-set

Description Configure a firewall rule-set.

This rule-set is also referred to as Access Control rule-set. It controls the traffic by permitting or denying the packets. It also controls logging, decides how traffic is forwarded, and includes packet rewrite functions like NAT.

Syntax

```
[no] rule-set name
```

Parameter	Description
rule-set *name*	Create a new firewall rule-set. Use fw active-rule-set to make a firewall rule-set active.

Default No default name for new rule-sets.

Mode Global configuration mode

NOTE: You can configure multiple Access Control as well as Traffic Control rule-sets. However, each type can have only one active rule-set at a time.

Example The following example shows creation of the rule-set called “new-DCfirewall-ruleset1”:

```
ACOS(config)# rule-set new-DCfirewall-ruleset1
ACOS(config-rule set:new-DCfirewall-r)#
```

remark

Description Configure notes for this rule-set.

Syntax

```
[no] remark notes
```

Parameter	Description
notes	Enter notes or remarks for this rule set. Notes can range from 1-255 characters.

Mode Rule-set configuration mode.

Default There are no remarks configured by default.

rule

Description Configure a rule within the Access Control rule-set and change the position of that rule within the rule-set.

Syntax

```
[no] rule name
[insert-rule
{top | before target-rule | after target-rule | bottom}]
```

Parameter	Description
name	Enter the name of the rule. This can range from 1-63 characters.
insert-rule	Add a rule to a rule-set in a designated position: By default, new rules are inserted at the bottom of the list, meaning they will be ignored if traffic matches a request that appears higher up in the rule-set. You can insert a rule into one of the following specific positions: • **top** – inserts the rule at the top position within the rule-set. • **before target-rule** – inserts the rule before a designated rule in the rule-set. • **after target-rule** – inserts the rule after a designated rule in the rule-set. • **bottom** – inserts the rule at the bottom position in the rule-set.

Default There are no rules configured by default.

Mode Rule-set configuration mode.

Usage The normal form of this command creates a new rule or edits an existing rule within a rule-set. The **no** form of this command removes an existing rule.

This command changes the CLI to the configuration level for the rule, where the following sub-commands are available.

Commands under rule-set rule	Description and Sub-commands
[no] **action** {**permit** | **deny** | **reset**}	Action to be performed on the policy. Can be one of the following: • **permit** – permits the session, and optionally forwards the packet. • **deny** [**log**] – denies the session. • **reset** [**log**] – resets the session.
[no] **application** { **any** | **category** | **object-group** | **protocol** }	For Application Aware Firewall, configures application match condition in a security policy rule-set. Can be any one of the following: • **any** – Any application. • **category** – Specify application category. • **object-group** –Specify object group of the application. • **protocol** – Specify one or more applications
[no] **dest** [**geolocation** [**list** *<name>*| **entry**] **black-list**] [**domain-list** *<name>*] {**ipv4-address** [*ip-addr* | **any**] | **object** *obj-name* | **object-group** *grp-name*| **server** *srv-name* |	Configure the destination match conditions, which can be one of the following: • **geolocation list** *<name>* - Pre-configured geolocation list name. • **geolocation entry** - Custom geolocation entry defined by user. • **black-list** - Black list the geolocation entry or geolocation list. • **domain-list** *<name>* - Pre-defined domain list name. • **ipv4-address** – *ip-addr* can be an ipv4-address or **any**. • **object** – specify the name of the network object.

Commands under rule-set rule	Description and Sub-commands
virtual-server *srv-name* | **zone** [**any** | *zone-name*]}	• **object-group** – specify the name of the network object group. • **server** – specify the real server name. • **virtual server** – specify the virtual server name. • **zone** – bind the zone for destination matching. **NOTE:** ACOS supports the ability to configure multiple SRC/DST hosts, subnets, objects, object-groups, and services within a single rule. However, only one source/destination zone can be configured per rule.
[**no**] **dscp** {*dscp-value* | **range** *dscp-start dscp-end*}	Configure the DSCP (Differentiated Services Code Point) match conditions, which can be one of the following: *dscp-value* - Enter a number (0-63) or specify any one of the following: • default - Default dscp (000000) • af11 - AF11 dscp (001010) • af12 - AF12 dscp (001100) • af13 - AF13 dscp (001110) • af21 - AF21 dscp (010010) • af22 - AF22 dscp (010100) • af23 - AF23 dscp (010110) • af31 - AF31 dscp (011010) • af32 - AF32 dscp (011100) • af33 - AF33 dscp (011110)

Commands under rule-set rule	Description and Sub-commands
	• af41 - AF41 dscp (100010) • af42 - AF42 dscp (100100) • af43 - AF43 dscp (100110) • cs1 - CS1 (precedence 1) dscp (001000) • cs2 - CS2 (precedence 2) dscp (010000) • cs3 - CS3 (precedence 3) dscp (011000) • cs4 - CS4 (precedence 4) dscp (100000) • cs5 - CS5 (precedence 5) dscp (101000) • cs6 - CS6 (precedence 6) dscp (110000) • cs7 - CS7 (precedence 7) dscp (111000) • ef - EF dscp (101110) **range** - You can specify the range (0-63) by providing *dscp-start* and *dscp-end* values.
[**no**] **idle-timeout** *num*	Enter *num* for the TCP/UDP idle-timeout. This value can range from 1-2097151 seconds. ACOS offers the ability to configure idle-timeouts at the `rule` level, and also at the per-port level (for TCP/UDP protocols under the firewall session-aging template). This enhancement may be helpful for long-lived protocols used for backups or data replication, and it may help meet the needs of customers who require the ability to configure different TCP/UDP ports with different timeout values, or who need to be able to configure idle-timeout values under individual rules within a rule-set.

Commands under rule-set rule	Description and Sub-commands
	Port-based timeouts and rule-based idle-timeouts are only available for TCP and UDP, and can only be configured for destination ports.
[no] **ip-version** {**v4** | **v6**}	Set the IP version for this rule. • **v4** – designates this as an IPv4 rule. • **v4** – designates this as an IPv6 rule.
[no] **move-rule** { **top** | **before** *target-rule* | **after** *target-rule* | **bottom** }	Move a rule within a rule-set. By default, new rules appear at the bottom of the list, meaning they will be ignored if traffic matches a request that appears higher up in the rule-set. However, you can move a new rule into one of the following positions: • **top** – moves the rule to the top position in the rule-set. • **before***target-rule* – moves the rule before a designated rule in the rule-set. • **after***target-rule* – moves the rule after a designated rule in the rule-set. • **bottom** – moves the rule to the bottom position in the rule-set.
[no] **remark** *comment*	Enter a comment or remark about this rule. Can be 1-255 characters.
[no] **sampling-enable** {**all** | **hit-count**}	Enable baselining. Options are: • **all** – All • **hit-count** – Hit count

Commands under rule-set rule	Description and Sub-commands
[no] service { any | icmp [code | type] | icmpv6 [code | type] | object-group *name* | proto-id *num* | tcp {dst | src} | udp {dst | src} | sctp [template *name*] |}	Service for the rule-set can consist of one or more of the following options: • **any** – any • **icmp[code | type]** – Specify the Internet Control Message Protocol code. The ICMP Codes, ICMP Types, and ICMPv6 Types that can be used as match filters in a rule are described **Firewall Configuration Guide**. • **icmpv6** – Internet Control Message Protocol version 6 • **object-group** – Specify the service object-group name. • **proto-id** – Specify the protocol ID (1-255). • **tcp** – TCP. Specify **dst** or **src** and then specify the following sub-options: ◦ **eq***port-num* – Equal to the port number (1-65535). ◦ **gt***port-num* – Greater than the port number (1-65535). ◦ **lt***port-num* – Lower than the port number (1-65535). ◦ **range***port-num* – The starting port number (1-65535). • **udp** – UDP. Specify **dst** or **src** and then specify the following sub-options: ◦ **eq***port-num* – Equal to the port number (1-65535). ◦ **gt***port-num* – Greater than the port number

Commands under rule-set rule	Description and Sub-commands
	(1-65535). ◦ **lt***port-num* – Lower than the port number (1-65535). ◦ **range***port-num* – The starting port number (1-65535). • **sctp** – SCTP. Specify a SCTP template to be used.
[**no**] **source** [**geolocation** [**list** | **entry**] **black-list**] { **ipv4-address** [*ip-addr* | **any**] | **object** *obj-name* | **object-group** *grp-name*| **server** *srv-name* | **zone** [**any** | *zone-name*]}	Configure the source match conditions, which can be one or more of the following: • **geolocation list** - Pre-configured geolocation list. • **geolocation entry** - Custom geolocation entry defined by user. • **black-list** - Black list the geolocation entry or geolocation list. • **ipv4-address** – *ip-addr* can be an ipv4-address or **any**. • **object** – specify the name of the network object. • **object-group** – specify the name of the network object group. • **server** – specify the real server name. • **zone** – bind the zone for source matching
[**no**] **track-application**	For application aware firewall, enables application statistics.
enable	Enable this rule.
disable	Disable this rule.

Example The following example shows how to configure a rule-set “rs1” and with the rule called “new-rule” at the top of the list:

```
ACOS(config)# rule-set rs1
ACOS(config-rule set:rs1)# rule new-rule insert-rule top
ACOS(config-rule set:rs1-rule:new-rule)#
```

Example For application aware firewall, the following example shows how to enable application statistics:

```
ACOS(config)# rule-set rs rule rule-1 track-application
```

Example For application aware firewall, the following example shows how to configure application match condition:

```
ACOS(config)# rule-set rs rule rule-1 application any
```

Related Commands:

- rule-set rule action permit
- fw session-aging

rule-set rule action permit

Description Configure the actions permitted for the traffic matching the rule of a rule-set.

Syntax

```
action permit [listen-on-port | log | cgnv6 | forward | ipsec
]
```

Parameter	Description
`listen-on-port`	Configure the permitted action as listen on the port.
`log`	Enable logging.
`cgnv6 [log | lsn-lid | fixed-nat | static-nat | ds-lite [ lsn-lid inspect-payload]]`	Apply CGNv6 policy to the rule. Available options are: • `log` – Enable logging. • `lsn-lid` – Apply specified CGNv6 LSN LID.

Parameter	Description

	• **fixed-nat** – Apply CGNv6 Fixed NAT.
	• **static-nat** – Apply CGNv6 Static NAT.
	• **ds-lite** - Apply CGNv6 Dual Stack-Lite.
	  • **lsn-lid <1-1023>** – Apply the specified CGNv6 LSN LID.
	  • **inspect-payload** – Inspect the encapsulated payload (IPv4) while processing DS-Lite traffic.
	NOTE:
	• If only **cgnv6** is selected, a class-list must be configured and specified globally.
	• If **cgnv6 lsn-lid** is selected, then configuring a class-list is not required. If **cgnv6 fixed-nat** is selected, a Fixed NAT session will be created.
	• If **cgnv6 static-nat** is selected, a Static NAT session will be created.

forward {**listen-on-port** | **log**}	Configure the permitted action Forward. Available options are: • **listen-on-port** – Listen on port. • **log** – Enable logging.
ipsec *<VPN_IPsec _ name>*	Configure the permitted action IPsec. When this action is configured, the packets matching this rule are forwarded to the specified IPsec VPN tunnel. The rate-limit policy is supported for this

Parameter	Description
	action in action-group.

Usage For Firewall-only mode, use the following options to configure the behavior of traffic matching the rule:

- **action permit**
- **action permit** [**log** | **listen-on-port**]
- **action permit forward**
- **action permit forward** [**lid** | **log** | **listen-on-port**]
- **action permit ipsec**

Usage For GiFW mode, use the following options to configure the behavior of traffic matching the rule:

- **action permit cgnv6**
- **action permit cgnv6 lsn-lid** [**log**]
- **action permit cgnv6 ds-lite lsn-lid 1 inspect-payload** [**log**]
- **action permit cgnv6 fixed-nat** [**log**]
- **action permit cgnv6 static-nat** [**log**]
- **action permit cgnv6 log**

rule-set rule action-group permit

Description Configure the action-group permitted for the traffic matching the rule of a rule-set.

Syntax

```
action-group permit [cgnv6 | forward | ipsec | limit-policy |
listen-on-port | log | respond-to-user-mac | set-dscp | tcp
syn-cookie]
```

Parameter	Description
cgnv6 [**lsn-lid** | **fixed-nat**]	Apply CGNv6 policy to the rule. Available options are: **lsn-lid** – Apply specified CGNv6 LSN LID. **fixed-nat** – Apply CGNv6 Fixed NAT. **Note**:

Parameter	Description
	• If only **cgnv6** is selected, a class-list must be configured and specified globally. • If **cgnv6 lsn-lid** is selected, a configuring a class-list is not required. • If **cgnv6 fixed-nat** is selected, a Fixed NAT session will be created. • If **cgnv6 static-nat** is selected, a Static NAT session will be created.
forward	Configure the permitted action Forward.
ipsec*<VPN IPSec name>*	Configure the permitted action IPsec. When this action is configured, the packets matching this rule are forwarded to the specified VPN IPsec tunnel. The rate-limit policy is supported for this action.
limit-policy *<template_num>*	Configure the rules defined in the specified limit-policy template. **NOTE:** For advanced rate-limiting features, configure the rate limiting under the Traffic Control rule-set instead of Access Control rule-set.
listen-on-port	Configure the permitted action as listen on the port.
log	Enable logging. The permit log command enables logging for a particular rule. The following commands when appended to permit log enable logging templates for a particular rule. • fw-logging-template <fw template name> • cgnv6-logging-template <CGNv6 template name> • netflow-monitor <monitor name>
respond-	Assigns the route hop based on the MAC address

Parameter	Description
to-user-mac	inside the client's request on the packets matching the rule. This option is disabled by default.
set-dscp *<dscp-value>*	Configure the DSCP (Differentiated Services Code Point) value to be set in the IP (IPv4 and IPv6) header. The following values are supported: • default - Default dscp (000000) • af11 - AF11 dscp (001010) • af12 - AF12 dscp (001100) • af13 - AF13 dscp (001110) • af21 - AF21 dscp (010010) • af22 - AF22 dscp (010100) • af23 - AF23 dscp (010110) • af31 - AF31 dscp (011010) • af32 - AF32 dscp (011100) • af33 - AF33 dscp (011110) • af41 - AF41 dscp (100010) • af42 - AF42 dscp (100100) • af43 - AF43 dscp (100110) • cs1 - CS1 (precedence 1) dscp (001000) • cs2 - CS2 (precedence 2) dscp (010000) • cs3 - CS3 (precedence 3) dscp (011000) • cs4 - CS4 (precedence 4) dscp (100000) • cs5 - CS5 (precedence 5) dscp (101000) • cs6 - CS6 (precedence 6) dscp (110000) • cs7 - CS7 (precedence 7) dscp (111000) • ef - EF dscp (101110)

Parameter	Description
	• <1-63> - The DSCP value. Enter a value in the range 0-63.
skip-urpf-check	Skip Unicast Reverse Path Forwarding check for the specified rule when the **fw urpf strict** command is configured. This ensures that hairpin traffic directed by router is permitted on the interface.
tcp syn-cookie { **enable** |**disable**} **tcp-half-openon-threshold** *<number>* **on-timeout** *<number>*	Configures TCP SYN cookie protection for the firewall rule. After enabling TCP SYN cookie, you can also specify a threshold and timeout value. The SYN cookie protection is triggered when the number of tcp-half-open sessions created by the traffic matching the rule exceed the specified threshold and is disabled after the timeout value expires. The default timeout value is 120 seconds. This configuration overrides the configuration of the `fw tcp syn-cookie` command. The following scenarios describe the behavior: • if `permit tcp syn-cookie` is disabled for a firewall rule, and the global `fw tcp syn-cookie` command is enabled with a specific threshold and timeout, ACOS does not consider the global configuration and disables syn-cookie protection for the traffic matching the rule. • if `permit tcp syn-cookie` is enabled for a firewall rule, and the global `fw tcp syn-cookie` command is also enabled with a specific threshold and timeout, ACOS does not consider the threshold and timeout for the traffic matching the rule. For this traffic, syn-cookie protection is always enabled.

Parameter	Description	
	NOTE:	This command cannot be configured when **fw allow-non-syn-session-create** command is enabled and vice versa.

Example The following example configures the action group with permit forward and limit-policy actions:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit forward
ACOS(config-rule set:r1-rule:1-action-group)# permit limit-
policy 1023
```

Example The following example configures the action group with permit cgnv6 fixed NAT actions:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit cgnv6
fixed-nat
```

Example The following example configures the action group with permit set DSCP actions:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit set-dscp
cs1
```

Example The following example configures multiple logging templates for a rule:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit log
ACOS(config-rule set:test-rule:1-acti...)# permit log fw-
logging-template fw_logging
ACOS(config-rule set:test-rule:1-acti...)# permit log cgnv6-
logging-template lsn_log
ACOS(config-rule set:test-rule:1-acti...)# permit cgnv6
ACOS(config-rule set:test-rule:1-acti...)# permit log netflow-
monitor
```

Example The following example configures tcp syn-cookie protection for a firewall rule, sets the threshold to 50 TCP half open sessions, and the timeout to 60 seconds:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit tcp syn-cookie enable tcp-half-open on-threshold 50 on-timeout 60
```

Example The following example configures the action group permitting the skip action for URPF checks:

```
ACOS(config-rule set:rs1)# rule cgn_to_fw_via_router
ACOS(config-rule set:rs1-rule:cgn_to_fw_v...)#action-group
ACOS(config-rule set:rs1-rule:cgn_to_fw_v...)#permit skip-urpf-check
ACOS(config-rule set:rs1-rule:cgn_to_fw_v...)#source ipv4-address 9.1.1.0/24
ACOS(config-rule set:rs1-rule:cgn_to_fw_v...)#source zone outside
ACOS(config-rule set:rs1-rule:cgn_to_fw_v...)#dest zone fw1
ACOS(config-rule set:rs1-rule:cgn_to_fw_v...)#dest ipv4-address any
```

rule-set rule action-group deny

Description Configure the deny action-group for the traffic matching the rule of a rule-set.

Syntax

```
deny [limit-policy  template_num | log]
```

Parameter	Description
limit-policy *template_num*	Specify the template limit policy number to be bound to the rule (of an access control rule-set). The rules or policies defined in the limit policy will be applied to all packets matching the rule. Binding the policy to the Deny rules allows the packets (that are being denied) to be tracked separately, thereby enabling early detection and mitigation of DDoS attacks.

Parameter	Description
	You can specify a value between 1 to 1023. **NOTE:** Only supported for Packets-Per-Second downlink traffic.
log	Enable logging. This command enables logging for a particular rule.

Default There are no rules/rule-sets configured by default.

Mode Rule-set rule configuration mode.

Example The following example configures the deny action group with limit-policy action:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# deny limit-policy 10
```

Example The following example configures the deny action group with logging action:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# deny log
```

rule-set rule action-group reset

Description Configure the reset action-group for the traffic matching the rule of a rule-set.

Syntax

```
reset [ limit-policy template_num | log | respond-to-user-mac ]
```

Parameter	Description
limit-policy *template_num*	Specify the template limit policy number to be bound to the rule (of an access control rule-set). The rules or policies defined in the limit policy will be applied to all packets matching the rule.

Parameter	Description
	Binding the policy to the Reset action allows the TCP sessions, that are being reset, to be tracked separately. You can specify a value between 1 to 1023. **NOTE:** Only supported for Packets-Per-Second downlink traffic.
log	Enable logging. This command enables logging for a particular rule.
respond-to-user-mac	Specify this option to assign the route hop based on the MAC address inside the client's request on the packets matching the rule.

Default There are no rules/rule-sets configured by default.

Mode Rule-set rule configuration mode.

Example The following example configures the reset action group with limit-policy action:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# reset limit-policy 10
```

Example The following example configures the reset action group with logging action:

```
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# reset log
```

sampling-enable

Description Enable sampling for the specified rule-set.

NOTE: See “Enabling Baselining and Rate Calculation” in the Command Line Reference for more information.

application

Description For Application aware firewall, configures application match condition in a security policy rule-set.

Syntax

```
application {any|category|object-group|protocol}
```

Parameter	Description
any	Any application.
category	Specify application category.
object-group	Specify object group of the application.
protocol	Specify one or more applications

Default Disabled

Mode Rule-set configuration

Example The following command applies the rule-set to any application:

```
ACOS(config)#rule-set rs rule rule-1 application any
```

track-application

Description Enable application statistic.

Syntax

```
track-application
```

Default Disabled

Mode Rule-set configuration

Example

```
rule-set rs rule rule-1 track-application
```

session-statistic

Description Enable or disable session-based statistics for the specified rule-set.

Syntax `session-statistic{enable | disable}`

Parameter	Description
enable	Enable session-based statistics for this rule-set.
disable	Disable session-based statistics for this rule-set.

Mode Rule-set configuration mode.

Example The following example shows how to enable session-based statistics for the rule-set, “r1”:

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# session-statistic enable
```

source

Description Enable or disable source configuration options or parameters for the specified rule-set.

Syntax `source {class_list | geo list | ipv4-address | ipv6-address | object | object-group | server | threat-list | zone} { <ipv4_address> | <ipv6_address> |<name> }`

Parameter	Description
class-list	Match source IP against class-list.
geo list	Geo-location list for filtering.
ipv4-address	IPv4 address of the selected option.
ipv6-address	IPv6 address of the selected option.
object	Pre-defined network object.
object-group	Pre-defined network object group.
server	SLB Real server name.
threat-list	Bind threat-list for source IP based filtering.

Parameter	Description
zone	Configure source zone.
name	Name of the selected option like geo-location list, object, object-group, server, threat list, or zone.
<ipv4-address>	IPv4 address of the selected option.
<ipv6-address>	IPv6 address of the selected option.

Mode Rule-set configuration mode.

Example The following example shows how to enable session-based statistics for the rule-set, “r1”:

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# source geo-list GEO_APAC1
ACOS(config-rule set:r1)# source threat-list APAC1
```

dest

Description Enable or disable destination configuration options or parameters for the
specified rule-set.

Syntax

```
dest {class_list | geo list | domain list | ipv4-address |
ipv6-address | object | object-group | server | threat-list |
zone} {<ipv4_address> | <ipv6_address> |<name> }
```

Parameter	Description
class-list	Match destination IP against class-list.
geo list	Geo-location list for filtering.
domain list	Domain name list for filtering at destination firewall.
ipv4-address	IPv4 address of the selected option.
ipv6-	IPv6 address of the selected option.

Parameter	Description
address	
object	Pre-defined network object.
object-group	Pre-defined network object group.
server	SLB Real server name.
threat-list	Bind threat-list for source IP based filtering.
zone	Configure destination zone.
name	Name of the selected option like geo-location list, object, object-group, server, threat list, or zone.
<ipv4-address>	IPv4 address of the selected option.
<ipv6-address>	IPv6 address of the selected option.

Mode Rule-set configuration mode.

Example The following example shows how to enable session-based statistics for the rule-set, “r1”:

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# dest geo-list GEO_APAC1
ACOS(config-rule set:r1)# dest threat-list APAC1
```

system radius server

Description Configure the interaction with firewall RADIUS servers for firewall commands.

Syntax

```
[no] system radius server
```

This command changes the CLI to the configuration level for the specified RADIUS server, where the following commands are available.

Command	Description
[no] accounting	Configures actions for RADIUS accounting messages. The following actions can be specified: • **interim-update** – Actions for accounting Interim-Update messages. The following options are available: **ignore**– Ignore the entry. **append-entry**– Append the AVPs to the existing entry. **replace-entry** – Replace the AVPs of the existing entry. • **on** – Actions for accounting On messages. • **delete-entries-using-attribute** – Delete entries matching attribute in RADIUS table. The following options are available: • **msisdn** – Clear using MSISDN • **imei** – Clear using IMEI • **imsi** – Clear using IMSI • **NAME<length:1-15>** – Clear using customized attribute • **ignore** – Ignore the request. • **start** – Actions for accounting Start messages. The following options are available: • **ignore**– Ignore the entry. • **append-entry**– Append the AVPs to the existing entry. • **replace-entry** – Replace the AVPs of the existing entry. • **stop** – Actions for accounting Stop messages.

Command	Description
	• **ignore**– Ignore the entry. • **delete-entry**– Delete the entry.
[**no**] **attribute** *attr-name* [[**vendor** *vendor-id*] **number** *attr-id*]	Specifies the client RADIUS attributes for the ACOS device to receive in response to RADIUS Accounting requests. The following attributes can be specified: • **inside-ipv6-prefix prefix-length** *num* – Framed IPv6 address. Specify the prefix-length for the Framed IPv6 address. • **inside-ip** – Inside client's IPv4 address. • **inside-ipv6** – Inside client's IPv6 address. • **imei** – Inside client's mobile number, as International Mobile Equipment Identity (IMEI). • **imsi** – Inside client's mobile number, as International Mobile Subscriber Identity (IMSI). • **msisdn** – Inside client's mobile number, as Mobile Station International ISDN Number (MSISDN). • **custom1**, **custom2**, **custom3**, **custom4 custom5**, **custom6** – Additional attributes not covered by other options. The vendor-id specifies the RADIUS vendor ID and can be 1-65535. The attr-id specifies the RADIUS attribute number and can be 1-255. These options, in combination, allow you to specify any attribute to be used as the client's inside IP address, or MSIDSN, or IMEI, and so on. For example, if your RADIUS server normally sends the MSIDSN attribute as attribute 31, you could use the following command to configure the ACOS device to use the same attribute value for MSIDSN: **attribute msisdn number 31**

Command	Description
[no] **derived-attribute [usergroup | userid] attribute { imei | imsi | msisdn | custom1-6 regex** *regular-expression* **}**	Specifies the derived attributes that are extended by the RADIUS attributes for the ACOS device to receive from external RADIUS servers in response to RADIUS Accounting requests. The following attributes can be specified: • **usergroup**– Configure the derived attributes of a user group. • **userid**– Configure the derived attributes of a user ID. The following attributes can be defined per usergroup or user ID: ○ **imei** – Inside client's mobile number, as International Mobile Equipment Identity (IMEI). ○ **imsi** – Inside client's mobile number, as International Mobile Subscriber Identity (IMSI). ○ **msisdn** – Inside client's mobile number, as Mobile Station International ISDN Number (MSISDN). ○ **custom1**, **custom2**, **custom3**, **custom4** **custom5**, **custom6** – Additional attributes not covered by other options *regex* – Specify a regular expression (1-127 characters) to parse the value from the RADIUS attribute. ACOS extracts the first matching substring based on the pattern specified. For example: ○ With the pattern ([^@]+) and the data as 'username@domain', ACOS extracts and stores the first sub-string 'username'.

Command	Description
	◦ With the pattern @(\w+) and the data 'username@domain', ACOS extracts and stores the first sub-string 'domain'. The regular expression supports the hexadecimal string. For example, ([^\x40]+) will be interpreted in the backend as ([^@]+), where \x40 represents the @ character in hexadecimal. **NOTE:** If the RADIUS start or interim-update accounting message does not contain a properly formatted value for a specified attribute, the backend receives an empty value for that attribute. This remains the case until the client sends a correctly formatted message, which is successfully received by ACOS.
no disable-reply	Specifies the toggle option for RADIUS reply packet. By default, the ACOS device sends the accounting responses to the RADIUS server.
[**no**] **listen-port** *portnum*	Specifies the port number on which the firewall RADIUS server listen for Accounting requests.
[**no**] **remote**	Specifies the name of the IP list that contains the IP addresses of the external RADIUS servers from which to obtain mobile numbers for traffic logging. The following options are available: **ip-list** – IP list of remote clients.
[**no**] **secret** *shared-secret*	Specifies the password string the external RADIUS servers and ACOS device use to authenticate RADIUS traffic between them.
[**no**] **vrid** *num*	Joins a VRRP-A failover group.

Default By default, no RADIUS servers are configured. When you use this command to configure one, the server has the defaults listed in the table above.

Mode Configuration mode

Usage You can configure ACOS to use the same mechanism for inserting the MSISDN values into HTTP request headers, that is used to insert the values into FW log messages.

Example The following example shows how to configure the **usergroup** and **userid** RADIUS derived attributes using regular expressions.

```
ACOS(config)#system radius server
ACOS(config-radius-server)#remote ip-list radius-client1
ACOS(config-radius-server)#attribute custom1 domain vendor
10101 number 41
ACOS(config-radius-server)#attribute inside-ip number 7
ACOS(config-radius-server)#attribute inside-ipv6 vendor 10101
number 28
ACOS(config-radius-server)#accounting start replace-entry
ACOS(config-radius-server)#derived-attribute usergroup
attribute custom1 regex @(\w+)
ACOS(config-radius-server)#derived-attribute userid attribute
custom1 regex ([^@]+)
```

template gtp

Description Define a GTP template.

Syntax `[no] template gtp {default | name}`

Parameter	Description
gtp-filter-list {*name*}	Specify a GTP filter list to be used for the given GTP template.
log {information-filtering | message-filtering}	Configure logging of packet drop based on information filtering or message filtering mechanism.

Parameter	Description
mandatory-ie-filtering {disable}	Disable GTP mandatory information element filtering.
maximum-message-length {*num*}	Specify the maximum message length for GTP messages.
message-type gtp-v2 {*options*}	Configure GTP message filtering based on the message types to be dropped/denied.
protocol-anomaly-filtering {disable}	Disable GTP anomaly filtering.
tunnel-timeout {*seconds*}	Configure the idle timeout for GTP sessions. The default is 5 minutes.

Default None

Mode Global configuration mode

Usage The following types of messages are supported under the **message-type gtp-v2** {*options*}:

The **gtp-v0 and gtp-v1** message types are:

- **bearer-resource** — Bearer Resource Command/Failure
- **change-notification** — Change Notification Request/Response
- **context** — Context Request/Response/Ack
- **config-transfer** — Configuration Transfer Tunnel
- **create-bearer** — Create Bearer Request/Response
- **create-data-forwarding** — Create Indirect Data Tunnel Request/Response
- **create-tunnel-forwarding** — Create Forwarding Tunnel Request/Response
- **create-session** — Create Session Request/Response
- **cs-paging** — CS Paging Indication
- **delete-bearer** — Delete Bearer Request/Response
- **delete-command** — Delete Bearer Command/Failure
- **delete-data-forwarding** — Delete Indirect Data Tunnel Request/Response

- **delete-pdn** — Delete PDN Connection Request/Response
- **delete-session** — Delete Session Request/Response
- **detach** — Detach Notification/Ack
- **downlink-notification** — Downlink Data Notification/Ack/Failure
- **echo** — Echo Request/Response
- **fwd-access** — Forward Access Context Notification/Ack
- **fwd-relocation** — Forward Relocation Request/Response/Complete
- **identification** — Identification Request/Response
- **mbms-session-start** — MBMS Session Start Request/Response
- **mbms-session-stop** — MBMS Session Stop Request/Response
- **mbms-session-update** — MBMS Session Update Request/Response
- **modify-bearer** — Modify Bearer Request/Response
- **modify-command** — Modify Bearer Command/Failure
- **release-access** — Release Access Bearer Request/Response
- **relocation-cancel** — Relocation Cancel Request/Response
- **resume** — Resume Notification/Ack
- **stop-paging** — Stop Paging Indication
- **suspend** — Suspend Notification/Ack
- **trace-session** — Trace Session Activation/Deactivation
- **update-bearer** — Update Bearer Request/Response
- **update-pdn** — Update PDN Connection Request/Response
- **version-not-supported** — Version Not Supported

template gtp-filter-list apn

Description Configure APN and IMSI filter list for GTP sessions.

Syntax

```
[no] template gtp-filter-list name apn name {imsi num|
selection-mode options}
```

Parameter	Description
imsi *num*	Set the International Mobile Subscriber

Parameter	Description
	Identity (IMSI) number as a filter to block traffic from a country or a region.
selection-mode {mobilestation | network | verified} [**imsi** *num*]	Specify the selection mode to block traffic based on the source of the APN. The following options are available: • **mobilestation** – Mobile station-provided APN, subscription not verified. • **network** – Network-provided APN, subscription not verified. • **verified** – MS or Network-provided APN, subscription verified.

Default None

Mode Global configuration mode

template gtp general-policy

Description The **template gtp general-policy** command places the CLI in template-general-policy configuration mode for modifying the specified gtp general-policy template. The command creates the template it is not extant.

A gtp general-policy template specifies GTP processing parameters for firewalls to which the template is bound.

Syntax

```
[no] template gtp general-policy TEMPLATE-LABEL
```

The **no template gtp general-policy** command deletes the specified gtp general-policy template and all commands configured within the template.

Mode Global configuration mode

Related Commands The following commands are available in **template-GTP-general-policy** configuration mode.

- gtp-version v0 permit

- maximum-message-length
- tunnel-timeout

Example This example places the CLI in template-GTP-general-policy configuration mode for to modifying the NAME-030 general-policy template.

```
ACOS(config)# template gtp general-policy NAME-030
ACOS(config-gtp-general-policy)# exit
ACOS(config)# show run | sec gtp
template gtp general-policy NAME-030
ACOS(config)#
```

template gtp logging-policy

Description The **template gtp logging-policy** command places the CLI in template-GTP-logging-policy configuration mode for modifying the specified gtp logging policy template. The command creates the template it is not extant.

A gtp logging-policy template specifies the events logged when packets are dropped by firewalls to which the template is bound. The related commands describe logging events that are available for logging.

Syntax

```
[no] template gtp logging-policy TEMPLATE-LABEL
```

The **no template gtp logging-policy** command deletes the specified gtp logging policy template and all commands configured within the template.

Mode Global configuration mode

The following commands are available in **template-gtp-logging-policy** configuration mode.

- log

The **exit** command returns the CLI to Global configuration mode.

Example This example places the CLI in template-GTP-logging-policy configuration mode for to modifying the NAME-050 logging-policy template.

```
ACOS(config)# template gtp logging-policy NAME-050
ACOS(config-gtp-logging-policy)# exit
ACOS(config)# show run | sec gtp
template gtp logging-policy NAME-050
ACOS(config)#
```

template gtp msisdn-list

Description The **template gtp msisdn-list** command places the CLI in template-GTP-msisdn configuration mode for modifying the specified gtp msisdn template. The command creates the template it is not extant.

A gtp msisdn-list template defines the list of mobile subscriber ISDN numbers that trigger the drop of packets by firewalls to which the template is bound.

Syntax

```
[no] template gtp msisdn-list TEMPLATE-LABEL
```

TEMPLATE-LABEL - the name of the gtp msisdn template.

The **no template gtp msisdn-list** command deletes the specified gtp msisdn template and all commands configured within the template.

Mode Global configuration mode

The following commands are available in **template-GTP-msisdn-list** configuration mode.

- msisdn

The **exit** command returns the CLI to Global configuration mode.

Example This example places the CLI in template-GTP-msidsn-list configuration mode for to modifying the NAME-070 msidsn-list template.

```
ACOS(config)# template gtp msisdn-list NAME-070
ACOS(config-gtp-msisdn-list)# exit
ACOS(config)# show run | sec gtp
template gtp msisdn-list NAME-070
ACOS(config)#
```

template gtp rate-limit-policy

Description The **template gtp rate-limit-policy** command places the CLI in template-GTP-rate-limit-policy configuration mode for modifying the specified gtp rate-limit-policy template. The command creates the template it is not extant.

A gtp msisdn-list template defines maximum number of specified packets, per-second, that can be processed by firewalls to which the template is bound. The related commands describe the packets for which rate limits can be imposed.

Syntax

```
[no] template gtp rate-limit-policy TEMPLATE-LABEL
```

TEMPLATE-LABEL - The name of the gtp rate-limit-policy template.

The **no template gtp rate-limit-policy** command deletes the specified gtp rate-limit-policy template and all commands configured within the template.

Mode Global configuration mode

The following commands are available in **template-gtp-rate-limit-policy** configuration mode.

gtp-*-rate

The **exit** command returns the CLI to Global configuration mode.

Example This example places the CLI in template-GTP-rate-limit-policy configuration mode for to modifying the NAME-080 rate-limit-policy template.

```
ACOS(config)# template gtp rate-limit-policy NAME-080
ACOS(config-gtp-rate-limit-policy)# exit
ACOS(config)# show run | sec gtp
template gtp rate-limit-policy NAME-080
```

template gtp-policy

Description The **template gtp-policy** command places the CLI in template-GTP-policy configuration mode for modifying the specified gtp policy. The

command creates the template it is not extant.

A GTP-Policy, when bound to a firewall rule set, specifies the GTP sub-policies that define GTP firewall behavior.

Syntax

```
[no] template gtp-policy TEMPLATE-LABEL
```

***TEMPLATE-LABEL* - The name of the gtp-policy template.**

The **no template gtp-policy** command deletes the specified gtp -policy template and all commands configured within the template.

Mode Global configuration mode

The following commands are available in **template-gtp-policy** configuration mode.

gtp

The **exit** command returns the CLI to Global configuration mode.

Example This example places the CLI in template-GTP-rate-limit-policy configuration mode for to modifying the NAME-080 rate-limit-policy template.

```
ACOS(config)# template gtp-policy NAME-300
ACOS(config-gtp-policy)# exit
ACOS(config)# show run | sec gtp
template gtp-policy NAME-300
```

template limit-policy

Description Create a template limit-policy to configure rate limiting.

Rate limiting helps to limit the traffic coming from certain application protocols and categories. It also ensures that the firewall operations are not interrupted, and the subscriber's connectivity is preserved.

NOTE: Rate limiting is supported for both, Gi firewall and transparent firewall.

Syntax

```
[no] template limit-policy num
```

Specify the limit policy number (1 to 1023).

This command changes the CLI to the configuration level that allows you to configure the specified limit policy using the following commands and parameters:

Parameter	Description
[no] limit-concurrent-sessions *num* **log**	Configure the limit for the maximum number of concurrent sessions. Concurrent Sessions are the total number of simultaneous sessions allowed at any time, per subscriber IP or subnet. Specify the concurrent session limit number (1 to 2147483647). **log** - Enable logging when the configured limit exceeds.
[no] limit-cps *num* **[burstsize** *bucket_size* **| relaxed]**	Configure the Connections Per Second (CPS) limit. CPS is the maximum number of connections that can be established per second, per subscriber IP or subnet. Specify the CPS threshold limit (1 to 2147483647). **burstsize** - Specify the token bucket size (1 to 2147483647) for CPS. It indicates the maximum number of tokens allowed to accumulate and hence the maximum burst size of the traffic that can be allowed. The size must exceed the configured CPS limit. **NOTE**: A template limit-policy that belongs to a rate-limit hierarchy and is not its root must not have a burstsize specified for any metric. **relaxed** - See relaxed.
[no] limit scope	Specify the scope for rate limiting. The following options are available: • **aggregate** - The rate limiting policy is applied on the traffic at a rule level.

Parameter	Description
	• **subscriber-ip** - The rate limiting policy is applied at a subscriber IP level defined in the rule. • **subscriber-prefix** *prefix_len* - The rate limiting policy is applied at a subscriber prefix level. It is applied to an entire subnet, instead of a single subscriber IP address. Specify the prefix length (1 to 128). • **radius attribute** - The rate limiting policy is applied at the level of the specified RADIUS attribute. It supports CPS, throughput, and concurrent sessions. For hierarchical rate-limiting, it only supports throughput and CPS. ACOS parses the value of this RADIUS attribute. The following attributes can be specified: ◦ **usergroup** - To apply rate-limit at the level of user group. ◦ **userid** - To apply rate-limit at the level of user ID. The default scope is **subscriber-ip** level. **NOTE**: For hierarchical rate-limiting, the scope of a parent template limit-policy cannot be more specific than that of a child.
[no] limit-pps	See template limit-policy limit-pps.
[no] limit-throughput	See template limit-policy limit-throughput.
parent *num*	Specify the parent template limit policy by entering the policy ID (1-1023). **NOTE**: The parent's id must not exceed that of the child.

Parameter	Description
	Specifying this option, places the template limit-policy in a rate-limit hierarchy. This causes the rate-limit entries based on this template limit-policy to be a part of a rate-limit hierarchy with the rate-limit entries based on the parent template limit-policy as their parent. **NOTE**: A template limit-policy that is a part of a rate-limit hierarchy cannot be bound to an Access Control rule. Additionally, only leaf-level template limit-policies (i.e., template limit-policies that are not specified as **parent** by any other template limit-policy) can be bound to the Traffic Control rules.
max-min-fair	Enable resource distribution in a **max-min-fair** manner for a hierarchical rate-limiting model. When this option is configured, the parent template limit-policy tracks the token utilization of the children (template limit policies) and if a child is unlikely to use all of its fair-share, the parent distributes this child's excess tokens to its siblings that are capable of using more than their fair-share. This option applies to all the metrics from a template limit-policy.
relaxed	Configure this option to allow the rate-limit entry to access more resources (from the parent policy) than the configured limit. It works only for template limit-policies that are part of a hierarchy. **NOTE** - This option can only be specified as part of the limit-cps or limit-throughput command.
user-tag	Add a customized tag.

Default None

Mode Global configuration mode

Usage The template limit policy is designed to protect the network from volumetric attacks that attempt to exceed the network's processing capacity. When the rate limit exceeds the configured threshold, the packets are dropped by default.

A template limit-policy is bound to an Access Control or Traffic Control rule (with certain restrictions when the **parent** command is configured). The traffic matching this rule is rate-limited as per the configured template limit-policy.

NOTE: You can either configure throughput or PPS under the same template limit-policy. You cannot configure both. Additionally, PPS cannot be configured in a template limit-policy that is part of a rate-limit hierarchy or is directly bound to a Traffic Control rule.

Example The following command sets the rate limit for the number of connections per second along with the bucket size (to handle a burst in traffic):

```
ACOS(config)# template limit-policy 1023
ACOS(config-limit-policy)# limit-scope subscriber-prefix 24
ACOS(config-limit-policy)# limit-cps 1000  burstsize 1500

ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule 1
ACOS(config-rule set:r1-rule:1)# source ipv4-address
12.10.10.0/24
ACOS(config-rule set:r1-rule:1)# source zone any
ACOS(config-rule set:r1-rule:1)# dest ipv4-address
9.9.9.173/32
ACOS(config-rule set:r1-rule:1)# dest zone any
ACOS(config-rule set:r1-rule:1)# service any

ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit forward
ACOS(config-rule set:r1-rule:1-action-group)# permit limit-
policy 1023
```

Example The following commands demonstrate a simple hierarchical rate-limiting model. In this configuration, the **template limit-policy** *10* is the parent, whereas the **template limit-policy** *20* is the child.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate

ACOS(config)# template limit-policy 20
ACOS(config-limit-policy)# limit-scope subscriber-prefix 64
ACOS(config-limit-policy)# parent 10
```

Example The following example demonstrates **relaxed** command usage. In this configuration, a relaxed limit is enabled for the downlink throughput metric; however, a strict limit is set for the CPS metric:

```
ACOS(config)# template limit-policy 1
ACOS(config-limit-policy)# limit-throughput downlink 100
relaxed
ACOS(config-limit-policy)# limit-cps 10
```

Example The following example demonstrates **max-min-fair** command usage. In this configuration, the aggregate limit policy (template limit-policy 20) specifies the downlink throughput limit of 10Gbps. This template serves as a parent for the subscriber-level entry (template limit-policy 10). The **max-min-fair** tag in the parent template limit-policy ensures that the parent rate-limit entry monitors the resource utilization of the children entries and if a child is unlikely to use its entire fair-share, the unused part is allocated to other sibling entries who are capable of utilizing it.

```
ACOS(config)# template limit-policy  10
ACOS(config-limit-policy)# limit-throughput downlink  10240
ACOS(config-limit-policy)# limit-scope aggregate
ACOS(config-limit-policy)# max-min-fair

ACOS(config-limit)# template limit-policy  20
ACOS(config-limit-policy)# limit-scope subscriber-ip
ACOS(config-limit-policy)# parent  10
```

Example The following example demonstrates the **limit-scope radius attribute usergroup** command usage. This configuration sets a

throughput rate-limit of 10000 for a specific usergroup as identified by the RADIUS attribute.

```
ACOS(config)#template limit-policy 1
ACOS(config-limit-policy)#limit-throughput total 10000
ACOS(config-limit-policy)#limit-scope radius attribute
usergroup
```

For more examples, refer to the **Firewall Configuration Guide**.

template limit-policy limit-pps

Description Configure the Packets-Per-Second (PPS) limit. It is the maximum number of packets allowed per second.

When the number of packets-per-second crosses the configured threshold, the excessive packets are dropped.

Syntax

```
[no] template limit-policy  num
```

Specify the limit policy number (1 to 1023).

The command changes the CLI to the configuration level for the specified limit policy.

Enter, **limit-pps** and then configure the following parameters based on your requirement:

```
limit-pps [ downlink | total | uplink ] pps [ burstsize
bucket_size | ddos-protection-factor num]
```

Parameter	Description
[downlink | total | uplink] *pps*	Configure the PPS rate limit. The following options are available: • **downlink** - Downlink traffic • **uplink** - Uplink Traffic • **total** - Sum total of downlink and uplink traffic *pps* - Specify the PPS threshold limit (1 to

Parameter	Description
	2147483647).
burstsize *bucket_size*	Specify the token bucket size (1 to 2147483647 packets). It indicates the maximum number of tokens allowed to accumulate and hence the maximum burst size of the traffic that can be allowed. The size must exceed the configured PPS limit for the uplink traffic.
ddos-protection-factor *num*	Enable DDoS protection for downlink traffic only. It is enabled when the PPS rate exceeds a value, which is greater than the product of the PPS threshold limit and DDoS protection factor (*num*). DDoS protection helps to block individual IP addresses or a subnet in case of DDoS attack. Specify the multiplying factor (1 to 50).

Default None

Mode Global configuration mode

Usage The rate limit policy is bound to a rule and is applied based on the rate limiting scope configured for the traffic matching the rule.

Example The following commands configures the packets-per-second rate limit on the uplink, downlink, and the total traffic. The burst size is also configured to handle a burst in the traffic.

```
ACOS(config)# template limit-policy 1023
ACOS(config-limit-policy)# limit-scope subscriber-ip
ACOS(config-limit-policy)# limit-pps downlink 10000 burstsize
15000
ACOS(config-limit-policy)# limit-pps uplink 10000 burstsize
15000
ACOS(config-limit-policy)# limit-pps total 20000 burstsize
25000
```

template limit-policy limit-throughput

Description Configure the throughput limit. Throughput is the maximum gigabits allowed per second.

When the throughput crosses the configured threshold, the excessive packets are dropped.

Syntax

```
[no] template limit-policy num
```

Specify the limit policy number (1 to 1023).

The command changes the CLI to the configuration level for the specified limit policy.

Enter, **limit-throughput** and then configure the following parameters based on your requirement:

```
limit-throughput [ downlink | total | uplink ] throughput [
Mbps | Kbps | Gbps] [ burstsize bucket_size |  relaxed ]
```

Parameter	Description
[downlink | total | uplink]*throughput* **[Mbps | Kbps | Gbps]**	Configure the throughput rate limit. The following options are available: • **downlink** - Downlink traffic • **uplink** - Uplink Traffic • **total** - Sum total of downlink and uplink traffic *throughput* - Specify the throughput threshold limit. Enter a value in the range of 100Kbps to 10Tbps. You can specify one of the following units for the threshold limit: **Mbps** - Megabits per second (this is the default unit).

Parameter	Description
	Kbps - Kilobits per second. If this unit is specified, the minimum configurable value is 100 Kbps. **Gbps** - Gigabits per second. The maximum value is 10000 Gbps. **NOTE**: If you do not specify a unit while configuring the limit, the value is considered in Mbps.
burstsize *bucket_size* **[Mbps | Kbps | Gbps]**	Specify the token bucket size (1 to 100000 Mbps). It indicates the maximum number of tokens allowed to accumulate and hence the maximum burst size of the traffic that can be allowed. The burst size can be specified in Mbps (default), Kbps, or Gbps. **Note:** The size must exceed the configured throughput limit for the uplink, downlink, and total traffic.
relaxed	Configure this option to allow the rate-limit entry to access more resources (from the parent policy) than the configured limit. It works only for template limit-policies that are part of a hierarchy. **NOTE** - This option can only be specified as part of the limit-cps, limit-pps, or limit-throughput command.

Default None

Mode Global configuration mode

Usage The rate limit policy is bound to a rule and is applied based on the rate limiting scope configured for the traffic matching the rule.

Example The following commands configure the throughput rate limit on the uplink, downlink, and the total traffic in Mbps. The burst size is also configured to handle a burst in the traffic.

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-ip
ACOS(config-limit-policy)#limit-throughput downlink 50000
burstsize 55000
ACOS(config-limit-policy)#limit-throughput uplink 50000
burstsize 55000
ACOS(config-limit-policy)#limit-throughput total 100000
burstsize 150000
```

Example The following commands configure the throughput rate limit on the uplink, downlink, and the total traffic in Kbps.

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-prefix 24
ACOS(config-limit-policy)#limit-throughput downlink 200 Kbps
ACOS(config-limit-policy)#limit-throughput uplink 300 Kbps
ACOS(config-limit-policy)#limit-throughput total 600 Kbps
```

Example The following commands configure the throughput rate limit on the uplink, downlink, and the total traffic in Gbps.

```
ACOS(config)#template limit-policy1024
ACOS(config-limit-policy)#limit-scope subscriber-prefix 24
ACOS(config-limit-policy)#limit-throughput downlink 90 Gbps
burstsize 95 Gbps
ACOS(config-limit-policy)#limit-throughput uplink 90 Gbps
burstsize 95 Gbps
ACOS(config-limit-policy)#limit-throughput total 90 Gbps
burstsize 95 Gbps
```

template sctp

Description Define a SCTP template.

Syntax `[no] template sctp {default | name}`

Parameter	Description
checksum-check {enable}	Enable checksum check on SCTP packets.
half-open-idle-timeout {*seconds*}	Set SCTP half-open timeout in seconds.
idle-timeout {*minutes*}	Set SCTP idle timeout in minutes.
log {payload-proto-filtering}	Log Payload Protocol IDs Filtered.
permit-payload-protocol {iua | m2ua | m3ua | sua | m2pa | h.323}	Configure SCTP permitted payload protocols.

Default None

Mode Global configuration mode

traffic-control active-rule-set

Description Activate the specified Traffic Control rule-set in an application delivery partition. The rule-set must exist prior to activation.

Syntax `[no] traffic-control active-rule-set rule-set-name`

Default No default active rule-set

Mode Configuration mode

NOTE: It may take approximately 10 seconds for the rule-set to become active.

Example In the following example, the Traffic Control rule-set *tcrs1* is activated:

```
ACOS(config)# traffic-control active-rule-set tcrs1
```

traffic-control rule-set

Description Configure a Traffic Control rule-set.

This rule-set applies rate limiting policies to limit the network traffic. It also supports advanced features such as hierarchical rate-limiting.

Syntax

```
[no] traffic-control rule-set name
```

Parameter	Description
rule-set *name*	Create a new Traffic Control rule-set. Use **traffic-control active-rule-set** command to activate this rule-set.

Default No default name for new rule-sets

Mode Configuration mode

Example In the following example, the Traffic Control rule-set *tcrs1* is configured:

```
ACOS(config)# traffic-control rule-set tcrs1
ACOS(config-rule set:tcrs1)#
```

remark

Description Configure notes for this rule-set.

Syntax

```
[no] remark notes
```

Parameter	Description
notes	Enter notes or remarks for this rule set. Notes can range from 1-255 characters.

Mode Rule-set configuration mode.

Default There are no remarks configured by default.

rule

Description Configure a rule within a Traffic Control rule-set.

You can also change the position of the rule within the rule-set.

Syntax

```
[no] rule name
[insert-rule
{top | before  target-rule | after  target-rule | bottom}]
```

Parameter	Description
name	Enter the name of the rule. This can range from 1 to 63 characters.
insert-rule	Add a rule to a rule-set in a designated position: By default, new rules are inserted at the bottom of the list, meaning they will be ignored if traffic matches a request that appears higher up in the rule-set. You can insert a rule into one of the following specific positions: • **top** – inserts the rule at the top position within the rule-set. • **beforetarget-rule** – Inserts the rule before a designated rule in the rule-set. • **after target-rule** – Inserts the rule after a designated rule in the rule-set. • **bottom** – Inserts the rule at the bottom position in the rule-set.

Default There are no rules configured by default

Mode Traffic Control Rule-set configuration mode

Usage The regular form of this command creates a new rule or edits an existing rule within a rule-set. The **no** form of this command removes an existing rule.

This command changes the CLI to the configuration level for the rule, where the following sub-commands are available.

Commands under rule-set rule	Description and Sub-commands
[no] **action-group** [no] **action** **{ limit-policy** *num*}	Configure the action in the action group by specifying the rate limit policy.
[no] **dest [class-list** *<name>* **| domain-list** *<name>* **| geolocation [list <name>| entry] black-list] [domain-list** *<name>*] **{ipv4-address** [*ip-addr* **| any] | object** *obj-name* **| object-group** *grp-name*| **server** *srv-name* **| virtual-server** *srv-name* **| zone** [**any |** *zone-name*]}	Configure the destination match conditions, which can be one of the following: • **class list** *<name>* - Pre-configured class-list name. • **domain-list** *<name>* - Pre-configured domain-list name. • **geolocation list <name>** - Pre-configured geolocation list name. • **geolocation entry** - Custom geolocation entry defined by user. • **black-list** - Black list the geolocation entry or geolocation list. • **ipv4-address** – *ip-addr* can be an ipv4-address or **any**. • **object** – specify the name of the network object. • **object-group** – specify the name of the network object group. • **server** – specify the real server name. • **virtual server** – specify the virtual server name. • **zone** – bind the zone for destination matching.
[no] **ip-version** {**v4 | v6 |any**}	Set the IP version for this rule.

Commands under rule-set rule	Description and Sub-commands
	• **v4** – designates this as an IPv4 rule. • **v6** – designates this as an IPv6 rule. • **any** – used for handling both IPv4 and IPv6 traffic. This option is only compatible with filters by application, zone or the source class-list of the RADIUS type.
[no] **remark** *comment*	Enter a comment or remark about this rule. It can be 1-255 characters.
[no] **sampling-enable** {**all** | **hit-count**}	Enable baselining. Options are: • **all** – All • **hit-count** – Hit count
[no] **service** { **any** | **icmp** [**code** | **type**] | **icmpv6** [**code** | **type**] | **object-group** *name* | **proto-id** *num* | **tcp** {**dst** | **src**} | **udp** {**dst** | **src**} | **sctp** [**template** *name*] |}	Service for the rule-set can consist of one or more of the following options: • **any** – any • **icmp[code | type]** – Specify the Internet Control Message Protocol code. The ICMP codes, ICMP types, and ICMPv6 types that can be used as match filters in a rule are described **Firewall Configuration Guide**. • **icmpv6** – Internet Control Message Protocol version 6 • **object-group** – Specify the service object-group name. • **proto-id** – Specify the protocol ID (1-255). • **tcp** – TCP. Specify **dst** or **src** and then

Commands under rule-set rule	Description and Sub-commands
	specify the following sub-options: ◦ **eq***port-num* – Equal to the port number (1-65535). ◦ **gt***port-num* – Greater than the port number (1-65535). ◦ **lt***port-num* – Lower than the port number (1-65535). ◦ **range***port-num* – The starting port number (1-65535). • **udp** – UDP. Specify **dst** or **src** and then specify the following sub-options: ◦ **eq***port-num* – Equal to the port number (1-65535). ◦ **gt***port-num* – Greater than the port number (1-65535). ◦ **lt***port-num* – Lower than the port number (1-65535). ◦ **range***port-num* – The starting port number (1-65535). • **sctp** – SCTP. Specify a SCTP template to be used.
[**no**] **source [class-list** *name* **[type radius derived-attribute {usergroup | userid}] | geolocation [list | entry] black-list]{ ipv4-address** [*ip-addr*| **any]** |	Configure the source match conditions, which can be one or more of the following: • **class-list** - Pre-configured class-list. ◦ **type radius derived-attribute {usergroup | userid}** - The value from this derived-attribute is matched in the class-list.

Commands under rule-set rule	Description and Sub-commands
object *obj-name* | **object-group** *grp-name*| **server** *srv-name* | **zone** [**any** | *zone-name*]}	• **geolocation list** - Pre-configured geolocation list. • **geolocation entry** - Custom geolocation entry defined by user. • **black-list** - Black list the geolocation entry or geolocation list. • **ipv4-address** – *ip-addr* can be an ipv4-address or **any**. • **object** – specify the name of the network object. • **object-group** – specify the name of the network object group. • **server** – specify the real server name. • **zone** – bind the zone for source matching
enable	Enable this rule.
disable	Disable this rule.

Example

The following example shows how to configure a Traffic Control rule-set **tcrs1**, add a new rule **rule1** to it and bind this rule to a pre-configured limit policy:

```
ACOS(config)# traffic-control rule-set tcrs1
ACOS(config-rule set:tcrs1)# rule rule1
ACOS(config-rule set:tcrs1-rule:rule1)# source ipv4-address
any
ACOS(config-rule set:tcrs1-rule:rule1)# source zone any
ACOS(config-rule set:tcrs1-rule:rule1)# dest ipv4-address any
ACOS(config-rule set:tcrs1-rule:rule1)# dest zone any
ACOS(config-rule set:tcrs1-rule:rule1)# service any
ACOS(config-rule set:tcrs1-rule:rule1)# action-group
ACOS(config-rule set:tcrs1-rule:rule1-acti...)# action limit-
policy 5
```

Example The following example shows how to configure a rule at the top of the list:

```
ACOS(config)# traffic-control rule-set tcrs1
ACOS(config-rule set:tcrs1)# rule rule1 insert-rule top
ACOS(config-rule set:tcrs1-rule:rule1)#
```

Example The following example shows how to configure a Traffic Control rule-set `ruleset1` with the `policy1` rule taking the value from the `usergroup` RADIUS derived-attribute to match in the `policy_1` source class-list. The `ip-version` set to `any` ensures that the traffic-control rule-set handles both IPv4 and IPv6 addresses for the RADIUS usergroup:

```
ACOS(config)#class-list policy_1 string
ACOS(config-class list)#str policy_1

ACOS(config)#traffic-control rule-set ruleset1
ACOS(config-rule set:ruleset1)#rule policy1
ACOS(config-rule set:ruleset1-rule:polic...)#ip-version any
ACOS(config-rule set:ruleset1-rule:polic...)#source class-list
policy_1 type radius derived-attribute usergroup
```

zone

Description Configure a security zone.

Syntax

```
[no] zone name
```

After using this command to create a new zone, the following commands are available:

Parameter	Description
[no] zone *name*	Create a new zone.
[no] interface ***option***	The the following interface options are available: • `ethernet` *port-num* – The configured interface is a virtual or physical Ethernet port with port-num ID. The port ID takes a range of values that depends of

Parameter	Description
	the platform ACOS is running on. • `lif` *`logicalinterface-id`* – The configured interface is a logical interface in a Software Defined Network (SDN) or Overlay Network with interface-id ID. The logical interface ID takes a range of values from 1 to 128. • `trunk` *`num`* – The configured interface is a logical trunk interface of the ACOS device. The trunk interface ID associates the interface with a trunk group and takes a range of values from 1 to 4096. • `tunnel` *`num`* – The configured interface is a tunnel. The tunnel interface ID takes a range of values from 1 to 128. • `ve` *`ve-num`* – The configured interface is a virtual Ethernet Interface. The virtual Ethernet ID takes a range of values that depends of the platform ACOS is running on.
`[no] local-type`	Prior to ACOS 4.1.1, configuring a rule with a destination IP address which is that of the ACOS device (such as a VIP), required the destination zone to be zone type **`any`**. If the destination is the ACOS device itself, then the packet was not forwarded out the device and the resulting route lookup was empty. However, in ACOS 4.1.1 and later, you can send traffic to the ACOS device itself by configuring the **`local-type`** command as the destination zone criteria. Designating a zone as a “local zone” removes the ability to include interfaces, management interface, VLANs, tunnels, VEs, and trunks in that local zone. **Details:**

Parameter	Description
	• When configuring a local zone as the destination zone criteria, the destination IP address must be the IP address of the ACOS device. • Local zone is only available as part of the destination zone criteria configuration, and you cannot configure a local zone as the source zone criteria in rule-set rule. • If a standard zone has already been configured in a rule-set rule, it cannot later be changed to a local zone, or vice versa.
[no] vlan *vlan-id* to *vlan-id*	Configure a virtual LAN (VLAN) by replacing *vlan-id* with the ID of the VLAN (2-4094), followed by the to command. Then specify the *vlan-id* for the other vlan in this zone.

Default No default name for new zones.

Mode Global configuration mode

Usage A firewall zone acts can contain multiple interfaces, IP addresses, and subnets. It offers a more convenient way to bind and manage many interfaces under a firewall rule simultaneously.

NOTE: Do not create a zone with the name “any” or you will not be able to later delete it. This limitation exists because ACOS auto-creates an invisible zone called “any” (for internal purposes). This system-created zone will not appear in the output of the “show running” CLI command. However, if you manually create a zone called “any”, then the zone will be visible in the output, but because it has the same name as the system-generated zone, you will be unable to delete it.

Show Commands

show automatic-update

Description For application aware firewall, show command layout for automatic application firewall software update.

Syntax

```
show automatic-update
```

Mode All

Usage Use to check automatic update schedule and software version.

Example

```
ACOS(config:1)# show automatic-update
-------------------------------------------------------------------
-------------------------
Feature name         Version         Schedule          Time
Last Updated    Next Check
-------------------------------------------------------------------
-------------------------
app-fw               1.301.0-20       Daily               11:01
   N/A       2017-05-12
```

show counters fw alg

Description Display counters for various Application Layer Gateway (ALG) protocols.

Syntax

```
show counters fw alg { esp | ftp | pptp | rtsp | sip | tftp }
```

Parameter	Description
esp	Display counters related to Encapsulating Security Payload (ESP) ALG.

Parameter	Description
ftp	Display counters related to File Transfer Protocol (FTP) ALG.
pptp	**Display counters related to the Point-to-Point Tunneling Protocol (PPTP) ALG.**
rtsp	**Display counters related to the Real-Time Streaming Protocol (RTSP) ALG.**
sip	**Display counters related to the Session Initiation Protocol (SIP) ALG.**
tftp	**Displays counters related to the Trivial File Transfer Protocol (TFTP) ALG.**

Mode All

Example

```
ACOS(config)# show counters alg esp
show counters fw alg esp
-------------------------------------
ESP Sessions Created
  0
ESP Helper Sessions Created
  0
ESP Helper Sessions Freed
  0
```

Field	Description
ESP Sessions Created	**The total number of ESP sessions created.**
ESP Helper Sessions Created	**The number of helper sessions created to help manage ESP traffic.**
ESP Helper Sessions Freed	**The number of helper sessions freed.**

Example

```
ACOS(config)# show counters alg ftp
show counters fw alg ftp
---------------------------------------
PORT Requests From Client
  0
EPRT Requests From Client
  0
PASV Replies From Server
  0
EPSV Replies From Server
  0
```

Field	Description
PORT Requests From Client	The number of PORT commands received from FTP clients. This command is used by an FTP client to specify the IP address and port number for the data connection during FTP.
EPRT Requests From Client	The number of Extended PORT (EPRT) commands received from FTP clients. This command is an extended version of the PORT command and is used in IPv6 networks to specify the IP address and port number.
PASV Replies From Server	The number of Passive (PASV) replies received from FTP servers.
EPSV Replies From Server	the number of Extended Passive (EPSV) replies

Field	Description
	received from FTP servers.

Example

```
ACOS(config)# show counters alg pptp
show counters fw alg pptp
---------------------------------------
Calls Established
  0
Call ID Mismatch on Call Request
  0
Call ID Mismatch on Call Reply
  0
GRE Session Created
  0
GRE Session Freed
  0
```

Field	Description
Calls Established	**The number of PPTP calls (sessions) successfully established.**
Call ID Mismatch on Call Request	**The number of instances where there is a mis-match in Call IDs on PPTP call requests.**
Call ID Mismatch on Call Reply	**The number of instances where there is a mis-match in Call IDs on PPTP call replies.**
GRE Session Created	**The number of Generic Routing Encapsulation (GRE) sessions created. These sessions are used**

Field	Description
	to encapsulate PPTP data packets for network transmission.
GRE Session Freed	The number of GRE sessions created. When a PPTP session ends, the associated GRE session is also freed.

Example

```
ACOS(config)# show counters alg rtsp
show counters fw alg rtsp
--------------------------------------
Transport Created
  0
Transport Freed
  0
Transport Alloc Failure
  0
Data Session Created
  0
Data Session Freed
  0
```

Field	Description
Transport Created	The number of RTSP transport sessions created.
Transport Freed	The number of RTSP transport sessions freed.
Transport Alloc Failure	The number of failures encountered while allocating resources for RTSP transport sessions.

Field	Description
Data Session Created	**The number of RTSP data sessions created.**
Data Session Freed	**The number of RTSP data sessions freed.**

Example

```
ACOS(config)# show counters alg sip
show counters fw alg sip
---------------------------------------
Request Received
  0
Response Received
  0
Method REGISTER
  0
Method INVITE
  0
Method ACK
  0
Method CANCEL
  0
Method BYE
  0
Method OPTIONS
  0
Method PRACK
  0
Method SUBSCRIBE
  0
Method NOTIFY
  0
Method PUBLISH
  0
Method INFO
  0
Method REFER
  0
```

```
Method MESSAGE
  0
Method UPDATE
  0
Method Unknown
  0
```

Field	Description
Request Received	**The total number of SIP requests received.**
Response Received	**The total number of SIP responses received.**
Method REGISTER	**The number of REGISTER requests received.**
Method INVITE	**The number of INVITE requests received.**
Method ACK	**The number of ACK (acknowledgment) requests received.**
Method CANCEL	**The number of CANCEL requests received.**
Method BYE	**The number of BYE requests received.**
Method OPTIONS	**The number of OPTIONS requests received.**
Method PRACK	**The number of Pro-visional Acknowledgment (PRACK) requests received.**
Method SUBSCRIBE	**The number of SUBSCRIBE requests received.**
Method NOTIFY	**The number of NOTIFY requests received.**

Field	Description
Method PUBLISH	**The number of PUBLISH requests received.**
Method INFO	**The number of INFO requests received.**
Method REFER	**The number of REFER requests received.**
Method MESSAGE	**The number of MESSAGE requests received.**
Method UPDATE	**The number of UPDATE requests received.**
Method Unknown	**The number of requests received with unknown methods.**

Example

```
ACOS(config)# show counters alg tftp
show counters fw alg tftp
-------------------------------------
TFTP Client Sessions Created
  0
```

Field	Description
TFTP Client Sessions Created	**The number of TFTP client sessions created. This session is created when a client starts a file transfer process using the TFTP protocol.**

show counters fw ddos-protection

Description Display counters related to DDoS protection implemented by the firewall.

Syntax `show counters fw ddos-protection`

Mode All

```
ACOS(config)# show counters fw ddos-protection
****************************
Too many DDOS entries
0
DDOS entry added
0
DDOS entry removed
0
DDoS Entry added to BGP
0
DDoS Entry Removed from BGP
0
DDOS entry BGP remove failures
0
DDOS Packet Drop
0
```

Field	Description
Too many DDOS entries	The number of instances where the system has encountered an excessive number of DDoS entries.
DDOS entry added	The number of new DDoS entries added.
DDOS entry removed	The number of DDoS entries removed.
DDoS Entry added to BGP	The number of DDoS entries added to the Border Gateway Protocol (BGP) configuration.
DDoS Entry Removed from BGP	The number of DDoS entries removed from the BGP configuration.

Field	Description
DDOS entry BGP remove failures	The number of failures encountered while removing DDoS entries from the BGP configuration.
DDOS Packet Drop	The number of packets dropped by the DDoS protection mechanism.

show counters fw global

Description Display Firewall parameters.

Syntax `show counters fw global`

Mode All

Example The following example shows sample output for the **`show counters fw global`** command:

```
ACOS(config)# show counters fw global
TCP Full-cone Created                                    0
TCP Full-cone Freed                                      0
UDP Full-cone Created                                    0
UDP Full-cone Freed                                      0
Full-Cone Creation Failure                               0
Data Session Created                                     44
Data Session Created Local                               0
Data Session Freed                                       44
Data Session Freed Local                                 0
Dynamic Blacklist Session Created                        0
Dynamic Blacklist Freed                                  0
Dynamic Blacklist - Packet Drop                          0
Total Active Full-cone sessions                          0
Limit Entry Created                                      0
Limit Entry Marked Deleted                               0
Undetermined rule detected                               0
Non-SYN pkt forward allowed                              0
Forward Ingress Packets TCP                              0
```

```
Forward Egress Packets TCP                                  0
Reverse Ingress Packets TCP                                 0
Reverse Egress Packets TCP                                  0
Forward Ingress Bytes TCP                                   0
Forward Egress Bytes TCP                                    0
Reverse Ingress Bytes TCP                                   0
Reverse Egress Bytes TCP                                    0
Forward Ingress Packets UDP                                 0
Forward Egress Packets UDP                                  0
Reverse Ingress Packets UDP                                 0
Reverse Egress Packets UDP                                  0
Forward Ingress Bytes UDP                                   0
Forward Egress Bytes UDP                                    0
Reverse Ingress Bytes UDP                                   0
Reverse Egress Bytes UDP                                    0
Forward Ingress Packets ICMP                                0
Forward Egress Packets ICMP                                 0
Reverse Ingress Packets ICMP                                0
Reverse Egress Packets ICMP                                 0
Forward Ingress Bytes ICMP                                  0
Forward Egress Bytes ICMP                                   0
Reverse Ingress Bytes ICMP                                  0
Reverse Egress Bytes ICMP                                   0
Forward Ingress Packets OTHERS                              0
Forward Egress Packets OTHERS                               0
Reverse Ingress Packets OTHERS                              0
Reverse Egress Packets OTHERS                               0
Forward Ingress Bytes OTHERS                                0
Forward Egress Bytes OTHERS                                 0
Reverse Ingress Bytes OTHERS                                0
Reverse Egress Bytes OTHERS                                 0
Forward Ingress Packet size between 0 and 200               0
Forward Ingress Packet size between 201 and 800             0
Forward Ingress Packet size between 801 and 1550            0
Forward Ingress Packet size between 1551 and 9000           0
Forward Egress Packet size between 0 and 200                0
Forward Egress Packet size between 201 and 800              0
Forward Egress Packet size between 801 and 1550             0
Forward Egress Packet size between 1551 and 9000            0
Reverse Ingress Packet size between 0 and 200               0
```

```
Reverse Ingress Packet size between 201 and 800                 0
Reverse Ingress Packet size between 801 and 1550                0
Reverse Ingress Packet size between 1551 and 9000               0
Reverse Egress Packet size between 0 and 200                    0
Reverse Egress Packet size between 201 and 800                  0
Reverse Egress Packet size between 801 and 1550                 0
Reverse Egress Packet size between 1551 and 9000                0
```

show counters fw gtp

Description Display Firewall GTP counters.

Syntax

```
show counters fw gtp
```

Mode All

The following example shows sample output for the **show counters fw gtp** command:

```
ACOS(config)#show counters fw gtp
Create Session Request                          4
Create Session Response                         3
Path Management Message                         0
Delete Session Request                          0
Delete Session Response                         0
Reserved field set drop                         0
Tunnel ID Flag Incorrect                        0
Message Filtering Drop                          1
Resevered Information Element Field Drop        0
Mandatory Information Element Field Drop        0
Invalid TEID Drop                               0
Out Of State Drop                               0
Fast Conn Setup Attempt                         3
Out of Session Memory                           0
No Forward Route                                0
NO Reverse Route                                0
Invalid TEID Field                              0
Retransmitted Create Session Request            0
Retransmitted Delete Session Request            0
Message Filtering Drop                          1
Resevered Information Element Field Drop        0
```

```
Mandatory Information Element Field Drop          0
Out Of State Drop                                 0
```

show counters fw hw-accelerate

Description Display hardware forwarding statistics for firewall sessions.

Syntax

```
show counters fw hw-accelerate
```

Example The following command displays information related to firewall sessions accelerated to the hardware:

```
ACOS(config)# show counters fw hw-accelerate
show counters fw hw-accelerate
************************************
HW Entries Created                                4
HW Entry Creation Failed                          0
HW Entry Creation Failed - server down            0
HW Entry Creation Failed - max entries exceeded   0
HW Entries Freed                                  4
HW Entries Freed - opposite tuple entry aged-out  2
HW Entry Freed - no HW prog                       0
HW Entry Freed - no matched conn                  0
HW Entry Freed - no software entry                16
HW Entries Count                                  0
HW Entries Aged Out                               8
HW Entries Aged Out - idle timeout                8
HW Entries Aged Out - TCP FIN                     0
HW Entries Aged Out - TCP RST                     0
HW Entries Aged Out - invalid dst                 0
HW Entries Force HW Invalidate                    0
HW Entries Invalidate due to server down          0
TCAM Flows Created                                2
TCAM Flows Freed                                  2
TCAM Flow Count                                   0
```

The following table describes the fields in the show command output.

Field	Description
HW Entries Created	Total number of hardware entries created.
HW Entry Creation Failed	Total number of times creation of hardware entries failed.
HW Entry Creation Failed - server down	Number of times creation of hardware entries failed since the server was down.
HW Entry Creation Failed - max entries exceeded	Number of times creation of hardware entries failed since the maximum entry count exceeded.
HW Entries Freed	Total number of hardware entries freed.
HW Entries Freed - opposite tuple entry aged-out	Number of hardware entries freed since the opposite tuple entry aged-out.
HW Entry Freed - no HW prog	Number of hardware entries freed since a hardware function was unavailable.
HW Entry Freed - no matched conn	Number of hardware entries freed since no connection matched.
HW Entry Freed - no software entry	Number of hardware entries freed since the software entry was not available.
HW Entries Count	Total number of hardware entries.
HW Entries Aged Out	Total number of hardware entries that aged-out.
HW Entries Aged Out - idle timeout	Number of hardware entries that aged-out due to idle timeout.
HW Entries Aged Out - TCP FIN	Number of hardware entries that aged-out after receiving a TCP FIN packet.
HW Entries Aged Out - TCP RST	Number of hardware entries that aged-out after receiving a TCP RST packet.
HW Entries Aged Out - invalid dst	Number of hardware entries that aged-out due to an invalid destination address.
HW Entries Force HW Invalidate	Number of hardware entries invalidated forcefully.

Field	Description
HW Entries Invalidate due to server down	Number of hardware entries invalidated since the server was down.
TCAM Flows Created	Total number of TCAM flows created.
TCAM Flows Freed	Total number of TCAM flows freed.
TCAM Flow Count	Total number of TCAM flows.

show counters fw logging

Description Display Firewall logging counters.

Syntax `show counters fw logging`

Mode All

The following example shows sample output for the **`show counters fw logging`** command:

```
ACOS(config)#show counters fw logging

/fw/logging
************************************
Log Packet Sent
  0
Log Event Type Reset
  0
Log Event Type Deny
  0
Log Event Type Session Close
  0
Log Event Type Session Open
  0
Firewall Rule Not Logged
  0
Log Packets Dropped
  0
TCP Session Created
  0
```

```
TCP Session Deleted
  0
UDP Session Created
  0
UDP Session Deleted
  0
ICMP Session Deleted
  0
ICMP Session Created
  0
ICMPV6 Session Deleted
  0
ICMPV6 Session Created
  0
Other Session Deleted
  0
Other Session Created
  0
HTTP Request Logged
  0
HTTP Logging Invalid Format Error
  0
SCTP Session Created
  0
SCTP Session Deleted
  0
Log Event Type SCTP Inner Proto Filter
  0
iDDoS IP Entry Created
  0
iDDoS IP Entry Deleted
  0
Session Limit Exceeded
  0
```

show counters fw per-instance

Description Display dynamic firewall counters per VRID/User group.

Syntax `show counters fw per-instance`

Mode All

Example Sample output for **`show counters fw per-instance`** command:

```
ACOS(config)#show counters fw per-instance

show counters fw per-instance
-------------------------------------
key-name = instance-0
Data Session Created
  1
Data Session Freed
  1
TCP Full-cone Created
  0
TCP Full-cone Freed
  0
UDP Full-cone Created
  0
UDP Full-cone Freed
  0
Dynamic Blacklist Session Created
  0
Dynamic Blacklist Session Freed
  0
Dynamic Blacklist Packet Drop
  0
Dynamic Blacklist - Version Mismatch
  0
Dynamic Blacklist - Pkt Rate Low
  0
Dynamic Blacklist - Pkt Rate High
  0
------------------------

show counters fw per-instance
-------------------------------------
key-name = instance-1
```

```
Data Session Created
  0
Data Session Freed
  0
TCP Full-cone Created
  0
TCP Full-cone Freed
  0
UDP Full-cone Created
  0
UDP Full-cone Freed
  0
Dynamic Blacklist Session Created
  0
Dynamic Blacklist Session Freed
  0
Dynamic Blacklist Packet Drop
  0
Dynamic Blacklist - Version Mismatch
  0
Dynamic Blacklist - Pkt Rate Low
  0
Dynamic Blacklist - Pkt Rate High
  0
------------------------
```

Field	Description
key-name	The name or key of the instance.
Data Session Created	The number of data sessions created.
Data Session Freed	The number of data sessions freed.
TCP Full-cone Created	The number of TCP full-cone NAT sessions created.
TCP Full-cone Freed	The number of TCP full-cone NAT sessions freed.

Field	Description
UDP Full-cone Created	The number of UDP full-cone NAT sessions created.
UDP Full-cone Freed	The number of UDP full-cone NAT sessions freed.
Dynamic Blacklist Session Created	The number of dynamic blacklist sessions created.
Dynamic Blacklist Session Freed	The number of dynamic blacklist sessions freed.
Dynamic Blacklist Packet Drop	The number of packets dropped due to dynamic blacklisting.
Dynamic Blacklist - Version Mismatch	The number of dynamic blacklist events due to version mismatch.
Dynamic Blacklist - Pkt Rate Low	The number of dynamic blacklist events triggered by a low packet rate.
Dynamic Blacklist - Pkt Rate High	The number of dynamic blacklist events triggered by a high packet rate.

show counters fw rate-limit

Description Display Firewall rate-limiting entries.

Syntax

```
show counters fw rate-limit
```

Mode All

Example Sample output for **show counters fw rate-limit** command:

```
ACOS(config)# show counters fw rate-limit
show counters fw rate-limit
-----------------------------------
Total Memory Used For Rate-limiting (bytes)
  4194460
```

```
Number of Total Rate-limit Entries
  0
Number of Rate-limit Entries with Scope Aggregate
  0
Number of Rate-limit Entries with Scope IPv4 Address
  0
Number of Rate-limit Entries with Scope IPv6 Address
  0
Number of Rate-limit Entries with Scope Session ID
  0
Number of Rate-limit Entries with Scope IPv4 Prefix
  0
Number of Rate-limit Entries with Scope IPv6 Prefix
  0
Number of Parent Rate-limit Entries with Scope Aggregate
  0
Number of Parent Rate-limit Entries with Scope IPv4 Prefix
  0
Number of Parent Rate-limit Entries with Scope IPv6 Prefix
  0
Number of Rate-limit Entries Allocated Totally
  0
Number of Rate-limit Entries Freed Totally
  0
Number of Rate-limit Entries with Scope IP
  0
Number of Parent Rate-limit Entries with Scope IP
  0
```

Field	Description
Total Memory Used For Rate-limiting (bytes)	The total memory used for rate-limiting purpose (measured in bytes).
Number of Total Rate-limit Entries	The total number of rate-limit entries created.
Number of Rate-limit Entries with Scope Aggregate	The number of rate-limit entries with scope Aggreg-

Field	Description
	ate.
Number of Rate-limit Entries with Scope IPv4 Address	The number of rate-limit entries with scope IPv4 Address.
Number of Rate-limit Entries with Scope IPv6 Address	The number of rate-limit entries with scope IPv6 Address.
Number of Rate-limit Entries with Scope Session ID	The number of rate-limit entries with scope Session ID.
Number of Rate-limit Entries with Scope IPv4 Prefix	The number of rate-limit entries with scope IPv4 Prefix.
Number of Rate-limit Entries with Scope IPv6 Prefix	The number of rate-limit entries with scope IPv6 Prefix.
Number of Parent Rate-limit Entries with Scope Aggregate	The number of parent rate-limit entries with scope Aggregate.
Number of Parent Rate-limit Entries with Scope IPv4 Prefix	The number of parent rate-limit entries with scope IPv4 Prefix.
Number of Parent Rate-limit Entries with Scope IPv6 Prefix	The number of parent rate-limit entries with scope IPv6 Prefix.
Number of Rate-limit Entries Allocated Totally	The total number of rate-limit entries allocated.
Number of Rate-limit Entries Freed Totally	The total number of rate-limit entries freed.
Number of Rate-limit Entries with Scope IP	The total number of rate-limit entries with scope IP.
Number of Parent Rate-limit Entries with Scope IP	The number of parent rate-limit entries with scope IP.

show counters fw server

Description Display statistics for the specified firewall logging server.

Syntax

```
show counters fw server server_name
```

Mode All

Example Sample output for **show counters fw server** command:

```
ACOS(config)# show counters fw server fw_server1
****************************
Current connections                          0
Total connections                            0
Forward packets                              0
Reverse Packets                              0
Peak connections                             0
```

Field	Description
Current connections	The number of active connections to the firewall logging server.
Total connections	The total number of connections made to the firewall logging server.
Forward packets	The number of packets forwarded by the firewall logging server.
Reverse Packets	The number of packets sent in the reverse direction, i.e., from the destination back to the source, by the firewall logging server.
Peak connections	The maximum number of simultaneous connections made by the firewall logging server.

show counters fw service-group

Description Display statistics for the specified firewall service-group.

Syntax

```
show counters fw service-group server_name
```

Mode All

Example Sample output for **show counters fw service-group** command:

```
ACOS(config)# show counters fw service-group fw_sg1
****************************
Service selection fail drop                          0
Service selection fail reset                         0
Service peak connection                              0
```

Field	Description
Service selection fail drop	The number of times packets were dropped because the firewall service-group failed to select a service.
Service selection fail reset	The number of times connections were reset because the firewall service-group failed to select a service.
Service peak connection	The maximum number of simultaneous connections to the firewall service group.

show counters fw tcp syn-cookie

Description View statistics related to Firewall SYN-cookie protection.

Syntax

```
show counters fw tcp syn-cookie
```

Mode All

Example The following example shows sample output for **show counters fw tcp syn-cookie** command:

```
ACOS (config)# show counters fw tcp syn-cookie
SYN cookie SYN ACK Sent                              0
SYN cookie verification passed                       0
SYN cookie verification failed                       0
```

Field	Description
SYN cookie SYN ACK Sent	The number of SYN ACK pack-

Field	Description
	ets sent by the device using TCP SYN cookies.
SYN cookie verification passed	The number of times SYN cookie verification process succeeds.
SYN cookie verification failed	The number of times the SYN cookie verification process fails.

show counters fw tcp-window-check

Description View the number of packets dropped after TCP window checks feature is enabled.

Syntax

```
show counters fw tcp-window-check
```

Mode All

Example The following example shows sample output for **show counters fw tcp-window-check** command:

```
ACOS(config)# show counters fw tcp-window-check
packet dropped for outside of tcp window 327719254
```

show counters rule-set

Description Display the counters for the security policy rule-set.

Syntax

```
show counters rule-set <rule-set name>
```

Mode All

Usage Used to view the counter values for the security policy rule set.

Example

```
ACOS(config:1)# show counters rule-set test
show counters rule-set test
```

```
-------------------------------------
Unmatched drops counter             31561
Permitted counter                   140169
Denied counter                      0
Reset counter                       0
```

The following table provides the field descriptions:

Field	Description
Unmatched drops counter	The number of packets dropped since the criteria within the rules (of the rule-set) are not matched.
Permitted counter	The number of packets permitted by the rule-set rules.
Denied counter	The number of packets denied by the rule-set rules.
Reset counter	The number of times the TCP sessions are reset by the rule-set rules.

show counters rule-set rule

Description Display the counters for the specified rule in the security policy rule-set.

Syntax

```
show counters rule-set <rule-set name> rule <rule name>
```

Mode All

Usage Used to view the counter values for the firewall rule in the security policy rule set.

Example The following example shows sample output for the **`show counters rule-set rs1 rule 1`** command:

```
ACOS(config:1)# show counters rule-set rs1 rule 1
show counters rule-set rs1 rule 1
-------------------------------------
Hit counts
  0
```

```
Permitted bytes counter
  2000
Denied bytes counter
  0
Reset bytes counter
  0
Permitted packets counter
  100
Denied packets counter
  0
Reset packets counter
  0
Active TCP session counter
  40
Active UDP session counter
  0
Active ICMP session counter
  0
Active other protocol session counter
  0
TCP session counter
  0
UDP session counter
  0
ICMP session counter
  0
Other protocol session counter
  0
Active SCTP session counter
  0
SCTP session counter
  0
Last hit counts timestamp
  0
Rate Limit Drops
  0
SYN cookie SYN ACK sent
  30
```

```
SYN cookie verification passed
  30
SYN cookie verification failed
  0
TCP half open sessions matching the rule
  12
```

show counters sctp global

Description Display SCTP global counters.

Syntax

```
show counters sctp global
```

Mode All

Example The following example shows sample output for the **show counters sctp global** command:

```
ACOS(config)# show counters sctp global
SCTP Static NAT Session Created                    0
SCTP Static NAT Session Deleted                    0
SCTP Firewall Session Created                      0
SCTP Firewall Session Deleted                      0
Packet Error Drop                                  0
Out-of-state Packet Drop                           0
Maximum Multi-homing IP Addresses Drop             0
Multi-homing Remove IP Parameter Skip              0
Multi-homing IP Address Not Found Drop             0
Static NAT Config Not Found Drop                   0
Configuration Error Drop                           0
NAT Resource VRRP-A Standby Drop                   0
Invalid Fragmented Chunks Drop                     0
Disallowed Chunk Filtered                          0
Disallowed Packet Drop                             0
Rate-limit Drop                                    0
Standby Session Created                            0
Standby Session Create Failed                      0
Standby Session Updated                            0
Standby Session Update Failed                      0
Static NAT Config Not Found on Standby             0
```

```
Out of System Memory                                    0
Max Conn Extension Size                                 0
```

show counters template gtp-policy

Description Display counters at the GTP policy level.

Syntax **show counters template gtp-policy** *policy_name*

Mode All

Example The following example shows sample output for the **show counters template gtp-policy** command:

```
ACOS(config)# show counters template gtp-policy temp-gtp
Tunnel Counters
-----------------------------------------------
GTPv0-C Tunnel Created
GTPv0-C Half open tunnel created
GTPv0-C Tunnel Delete Request
GTPv0-C Tunnel Marked Deleted
GTPv0-C Tunnel Deleted
GTPv0-C Half open tunnel closed
GTPv1-C Tunnel Created
GTPv1-C Half open tunnel created
GTPv1-C Tunnel Delete Request
GTPv1-C Tunnel Marked Deleted
GTPv1-C Tunnel Deleted
GTPv1-C Half open tunnel closed
GTPv2-C Tunnel Created
GTPv2-C Half open tunnel created
GTPv2-C Tunnel Delete Request
GTPv2-C Tunnel Marked Deleted
GTPv2-C Tunnel Deleted
GTPv2-C Half open tunnel closed
GTP-U Tunnel Created
GTP-U Tunnel Deleted
GTPv0-C Tunnel Deleted with Restart/failure
GTPv1-C Tunnel Deleted with Restart/failure
GTPv2-C Tunnel Deleted with Restart/failure
```

```
Information Counters
--------------------------------------------
GTPv0-C Update PDP Context Response Unsuccessful
GTPv1-C Update PDP Context Response Unsuccessful
GTPv2-C Modify Bearer Response Unsuccessful
GTPv0-C Create PDP Context Response Unsuccessful
GTPv1-C Create PDP Context Response Unsuccessful
GTPv2-C Create Session Response Unsuccessful
GTPv2-C Piggyback Message
GTP Path Management Messages Received
Permit GTPv0-C Reserved Messages
Permit GTPv1-C Reserved Messages
Permit GTPv2-C Reserved Messages
GTPv2-C Load Control Info IEs in message exceeded 2
GTPv1-C PDU Notification Request Forward
GTPv1-C PDU Notification Reject Request Forward
GTPv0-C PDU Notification Request Forward
GTPv0-C PDU Notification Reject Request Forward
GTPv0-C APN/IMSI Filtering Skipped (No IMSI)
GTPv1-C APN/IMSI Filtering Skipped (No IMSI)
GTPv2-C APN/IMSI Filtering Skipped (No IMSI)
GTPv0-C MSISDN Filtering Skipped (No MSISDN)
GTPv1-C MSISDN Filtering Skipped (No MSISDN)
GTPv2-C MSISDN Filtering Skipped (No MSISDN)
GTPv0-C Packet With Dummy MSISDN Forwarded
GTPv1-C Packet With Dummy MSISDN Forwarded
GTPv2-C Packet With Dummy MSISDN Forwarded

Validation Policy Drop Counters
--------------------------------------------
Validation Drop: GTPv2-C Create Session Request with TEID
Validation Drop: GTPv1-C PDU Notification Request with TEID
Validation Drop: GTPv0-C PDU Notification Request with TEID
Validation Drop: GTP repeated IE count exceeded
Validation Drop: Reserved Header Field Set
Validation Drop: Tunnel Header Flag Not Set
Validation Drop: Invalid Flow Label in GTPv0-C Header
Validation Drop: Invalid TEID Value
Validation Drop: Out Of State GTP Message
Validation Drop: Mandatory IE Not Present
```

```
Validation Drop: Mandatory IE in Grouped IE Not Present
Validation Drop: GTPv1-C Message Out of Order IE
Validation Drop: Unexpected IE Present in Message
Validation Drop: Reserved IE Field Present
Validation Drop: Invalid GTP version
Validation Drop: Message Length Exceeded
Validation Drop: Cross Layer IP Address Mismatch
Validation Drop: Country Code Mismatch in IMSI and MSISDN
Validation Drop: GTP-U IP Address Spoofed
Validation Drop: GTP Bearer count exceeded max (11)
Validation Drop: GTPV2-C Wrong LBI in Create Bearer Request
Validation Drop: GTP-C Drop Since Handover In Progress
Validation Drop: GTPv0-C Reserved Message Drop
Validation Drop: GTPv1-C Reserved Message Drop
Validation Drop: GTPv2-C Reserved Message Drop
Validation Drop: Piggyback message invalid packet length
Validation Drop: piggyback message anomaly failed
Validation Drop: GTP-C Sequence number Mismatch
Validation Drop: GTPV0 -C conn Sequence number Buffer Full
Validation Drop: GTPV1-C conn Sequence number Buffer Full
Validation Drop: GTPV2-C conn Sequence number Buffer Full
Validation Drop: GTP-C Invalid IMSI Length Drop
Validation Drop: GTP-C Invalid APN Length Drop
Validation Drop: Protocol flag in Header Field not Set
Validation Drop: GTPV0-c Subscriber Attributes Missing
Validation Drop: GTPV1-c Subscriber Attributes Missing
Validation Drop: GTPV2-c Subscriber Attributes Missing
Validation Drop: GTPv0-C APN/IMSI Filtering Dropped (No APN)
Validation Drop: GTPv1-C APN/IMSI Filtering Dropped (No APN)
Validation Drop: GTPv2-C APN/IMSI Filtering Dropped (No APN)

Filtering Policy Drop Counters
----------------------------------------------
Filtering Drop: Message Type Not Permitted on Interface
Filtering Drop: APN IMSI Filtering
Filtering Drop: MSISDN Filtering
Filtering Drop: RAT Type Filtering
Filtering Drop: GTP in GTP Tunnel Present

Rate-limit Policy Drop Counters
```

```
-------------------------------------------
Rate-limit Drop: Maximum GTPv0-C Message rate
Rate-limit Drop: Maximum GTPv1-C Message rate
Rate-limit Drop: Maximum GTPv2-C Message rate
Rate-limit Drop: GTPv1-C Create PDP Request rate
Rate-limit Drop: GTPv2-C Create Session Request rate
Rate-limit Drop: GTPv1-C Update PDP Request rate
Rate-limit Drop: GTPv2-C Modify Bearer Request rate
Rate-limit Drop: GTP-U Tunnel Creation rate
Rate-limit Drop: GTP-U Uplink byte rate
Rate-limit Drop: GTP-U Uplink packet rate
Rate-limit Drop: GTP-U Downlink byte rate
Rate-limit Drop: GTP-U Downlink packet rate
Rate-limit Drop: GTP-U Total byte rate
Rate-limit Drop: GTP-U Total packet rate
Rate-limit Drop: GTP-U Concurrent Tunnels

Message Length Drop Counters
-------------------------------------------
GTPv0-C IE Length Exceeds Message Length
GTPv1-C IE Length Exceeds Message Length
GTPv2-C IE Length Exceeds Message Length
GTPv0-C Message Length Mismatch Across Layers
GTPv1-C Message Length Mismatch Across Layers
GTPv2-C Message Length Mismatch Across Layers
```

show counters threat-intel threat-list

Description Show the counters for the number of hits for the specified threat-list. This threat-list is configured using the Webroot threat categories.

NOTE: On Multi-PU platforms, the counters display aggregated values from PU1 and PU2.

Syntax **show counters threat-intel threat-list** *<list-name>*

Mode All

Example The following example shows the sample output for this command:

```
ACOS# show counters threat-intel threat-list mylist

show counters threat-intel threat-list mylist
--------------------------------------
Hits for spam sources                   23
Hits for windows exploits               0
Hits for web attacks                    0
Hits for botnets                        0
Hits for scanners                       0
Hits for dos attacks                    0
Hits for reputation                     0
Hits for phishing                       0
Hits for proxy                          0
Hits for mobile threats                 0
Hits for tor-proxy                      0
Total hits for threat-list              23
```

show counters threat-intel webroot-global

Description Show the global counters for the Webroot module.

NOTE: On Multi-PU platforms, the counters display aggregated values from PU1 and PU2.

Syntax

```
show counters threat-intel webroot-global
```

Mode All

Example The following example shows sample output for this command:

```
ACOS# show counters threat-intel webroot-global

show counters threat-intel webroot-global
--------------------------------------
Hits for spam sources                         24
Hits for windows exploits                     0
Hits for web attacks                          0
Hits for botnets                              0
Hits for scanners                             0
Hits for dos attacks                          0
```

```
Hits for reputation                              0
Hits for phishing                                0
Hits for proxy                                   0
Hits for mobile threats                          0
Hits for tor-proxy                               0
Number of lookups in RTU cache                   0
Number of lookups in database                    24
IP's not found in database or RTU cache          7643
```

show fw application

Description For application aware firewall, lists all 3000 or more protocols supported on ACOS application aware firewall.

Syntax

```
show fw application [category category_name]
```

Default NA

Mode NA

Example

```
ACOS#show fw application
Application                   Description     Categories
-------------------------------------------------------------
01net                         01net.com       web
050plus                       050 plus        instant-messaging-
and-multimedia-conferencing, voip
0zz0                          0zz0.com        web, file-
management
10050net                      10050.net       web, web-websites
10086cn                       10086.cn        web
104com                        104.com         web
1111tw                        1111.com.tw     web
114la                         114la.com       web
115com                        115.com         web, cdn
118114cn                      118114.cn       web
11st                          11st.co.kr      web, web-e-
commerce

ACOS#show fw application category ?
```

```
aaa                                              aaa
  adult-content                                  adult-content
  advertising                                    advertising
  all                                            all
  analytics-and-statistics                       analytics-and-
statistics
  anonymizers-and-proxies                        anonymizers-and-
proxies
  audio-chat                                     audio-chat
  basic                                          basic
  blog                                           blog
  cdn                                            cdn
  chat                                           chat
  classified-ads                                 classified-ads
  cloud-based-services                           cloud-based-
services
  database                                       database
  email                                          email
  enterprise                                     enterprise
  file-management                                file-management
  file-transfer                                  file-transfer
  forum                                          forum
  gaming                                         gaming
  internet-of-things                             internet-of-things
  mobile                                         mobile
  multimedia-streaming                           multimedia-
streaming
  networking                                     networking
  news-portal                                    news-portal
  peer-to-peer                                   peer-to-peer
  remote-access                                  remote-access
  scada                                          scada
  social-networks                                social-networks
  software-update                                software-update
  standards-based                                standards-based
  video-chat                                     video-chat
  voip                                           voip
  vpn-tunnels                                    vpn-tunnels
  web                                            web
  web-e-commerce                                 web-e-commerce
```

```
webmails                                        webmails
web-search-engines                              web-search-engines
web-websites                                    web-websites
```

show fw ddos-protection entries

Description Display DDoS protection entries. This command displays blocked IP addresses and prefixes.

Syntax

```
show fw ddos-protection entries
```

Example

```
ACOS(config)# show fw ddos-protection entries
IP Address   Prefix   Rule PPS Expiration   Hints
-----------------------------------------------
47.27.10.10   32       1    0    117          -
```

The following table provides the field descriptions:

Field	Description
IP Address	The IP address that is under attack.
Prefix	The prefix configured for the specified subscriber IP address or subnet.
Rule	The name of the firewall rule.
PPS	The number of packets-per-second (PPS) sent to the subscriber IP address.
Expiration	The expiration time starts decrementing as soon as the IP is blacklisted and gets automatically renewed if the blacklisted IP continues to be under attack.
Hints	This field indicates whether the IP entry is in **Remove-Wait** or **Time Multiplier** state.

show fw full-cone-sessions

Description View Firewall Full Cone session information.

Syntax

```
show fw full-cone-sessions
[ipv4-address  ipv-addr | ipv6-address  ipv6-addr]
```

Mode All

Usage Use this command to display full-cone sessions created for hairpinning in the firewall.

Example The following example shows sample output for the **show fw full-cone-sessions** command:

```
ACOS(config)# show fw full-cone-sessions
Firewall - Full-cone Sessions:
Prot Inside Address                      Outbnd Inbnd  CPU
Age
-----------------------------------------------------------------
-
UDP  100.100.100.1:9874                    0      0      8
0
UDP  100.100.100.1:9917                    0      0      7
120
UDP  100.100.100.1:9894                    0      0      6
60
UDP  100.100.100.1:9898                    0      0      10
60
UDP  100.100.100.1:9885                    0      0      8
60
UDP  100.100.100.1:9950                    1      0      7
-
UDP  100.100.100.1:9878                    0      0      1
0
```

The following table describes the fields in the command's output.

Field	Description
Prot	Session protocol
Inside Address	Private IP address of the client
Outbound	Number of outbound sessions

Field	Description
Inbound	Number of inbound sessions
CPU	ACOS CPU on which the session resides
Age	Number of seconds the session has been in effect. The symbol '-' indicates that the session is active i.e., aging hasn't started yet. However, **X** indicates that the session is inactive, and will reject any new inbound data sessions matching the full cone session.

show fw limit-entry

Description View Firewall rate limit information.

Syntax

```
show fw limit-entry
[ prefix4  ipv4-prefix | prefix6  ipv4-prefix | rule-name
rule-name ]
```

Parameter	Description
prefix4 *ipv4-prefix*	View limit entries for the specified IPv4 prefix.
prefix6 *ipv6-prefix*	View limit entries for the specified IPv6 prefix.
rule-name *rule-name*	View limit entries matching the specified firewall rule.

Example The following example shows sample out for the **show fw limit-entry** command:

```
ACOS(config)# show fw limit-entry
IP/IPv6 Prefix/Length                Rule Name    Current
Maximum
-------------------------------------------------------------
-----
```

```
2050::/64                                rule1        10
 10
Total Rate Limit Entries Shown:1
-
```

show fw logging-keywords

Description Show valid keywords for logging firewall custom messages.

For a list of valid keywords, see fw template logging command.

Syntax

```
show fw logging-keywords [session_created | session_deleted]
custom_string
```

Parameter	Description
session-created *custom_string*	Logging keywords for session creation events.
session-deleted *custom_string*	Logging keywords for session deletion events.

Mode All

Example The following example shows sample output for the **show fw logging-keywords session_created** command:

```
ACOS(config)#show fw logging-keywords session-created
$rule-name$                    Rule name
$proto-name$                   Protocol name
$src-ip$                       source IP
$src-port$                     Source port
$dst-ip$                       Destination IP
$dst-port$                     Destination port
$in-interface$                 Interface of the incoming packet
$out-interface$                Interface of the outgoing packet
$rule-set-name$                Rule Set Name
$partition-name$               Partition Name
$sesn-start-time$              Session start time
$sesn-start-time-epoch$        Session start time Epoch
$time-stamp$                   Log generation time stamp
```

```
$src-zone$                      Source Zone
$dest-zone$                     Dest Zone
$app-id$                        App Id
$radius-msisdn$                 RADIUS attribute: MSISDN
$radius-imei$                   RADIUS attribute: IMEI
$radius-imsi$                   RADIUS attribute: IMSI
$radius-ctm1$                   RADIUS attribute: Custom1
$radius-ctm2$                   RADIUS attribute: Custom2
$radius-ctm3$                   RADIUS attribute: Custom3
$radius-ctm4$                   RADIUS attribute: Custom4
$radius-ctm5$                   RADIUS attribute: Custom5
$radius-ctm6$                   RADIUS attribute: Custom6
ACOS(config)#
```

Example The following example shows sample output for the **`show fw logging-keywords session_deleted`** command:

```
ACOS(config)#show fw logging-keywords session-deleted
$rule-name$                     Rule name
$proto-name$                    Protocol name
$src-ip$                        source IP
$src-port$                      Source port
$dst-ip$                        Destination IP
$dst-port$                      Destination port
$in-interface$                  Interface of the incoming packet
$out-interface$                 Interface of the outgoing packet
$rule-set-name$                 Rule Set Name
$partition-name$                Partition Name
$sesn-start-time$               Session start time
$sesn-start-time-epoch$         Session start time Epoch
$sesn-end-time$                 Session end time
$sesn-end-time-epoch$           Session end time Epoch
$sesn-dur$                      Session duration
$time-stamp$                    Log generation time stamp
$src-zone$                      Source Zone
$dest-zone$                     Dest Zone
$app-id$                        App Id
$in-bytes$                      Incoming byte count
$out-bytes$                     Outgoing byte count
$pkts-tx$                       Packets Transmitted
$pkts-rx$                       Packets Received
```

```
$radius-msisdn$                 RADIUS attribute: MSISDN
$radius-imei$                   RADIUS attribute: IMEI
$radius-imsi$                   RADIUS attribute: IMSI
$radius-ctm1$                   RADIUS attribute: Custom1
$radius-ctm2$                   RADIUS attribute: Custom2
$radius-ctm3$                   RADIUS attribute: Custom3
$radius-ctm4$                   RADIUS attribute: Custom4
$radius-ctm5$                   RADIUS attribute: Custom5
$radius-ctm6$                   RADIUS attribute: Custom6
ACOS(config)#
```

show fw match

Description Display the firewall match results (for the given interface). The output provides information about the rule sets and the specific rules matched by traffic

Syntax

```
show fw match
```

Mode All

Example The following example shows sample output for the **show fw match** command:

```
ACOS(config-if:ethernet:2)# show fw match
Firewall - Match Result
Active Access Control Rule-Set: rs1
Active Traffic Control Rule-Set: None
Total Number of Matching Rules: 1
Matching Rules Fetched: 1
Matching Rule: r1, type Access-control
```

Field	Description
Active Access Control Rule-Set	The name of the currently active Access-control rule set.
Active Traffic Control Rule-Set	The name of the currently active Traffic-control rule

Field	Description
	set.
Total Number of Matching Rules	The total number of rules that matched the traffic.
Matching Rules Fetched	The number of matching rules being fetched.
Matching Rule	The name and type of the rule that matched the traffic. The rule set type can be either an Access-control or a Traffic-control.

show fw rate-limit

Description Display the received traffic and the configured limit for each rate-limit entry.

Syntax

```
show fw rate-limit [ string-value | summary | ipv4_address |
ipv6_address/nn | template-id num ]
```

Parameter	Description
string-value NAME	Display the rate limit information for the specified string value. The length of the string value can be 1-128 characters.
summary	Display a summary of the rate-limit entries.
ipv4_address	Display the rate limit information for the specified IPv4 address.
ipv6_address/nn	Display the rate limit information for the specified IPv6 address and prefix length.
template-id *num*	Display the rate limit information for the specified template limit policy ID (1-1023).
| *modifier*	This is an optional command that can be used to display a specific part of the output.

Example

```
ACOS(config)# show fw rate-limit

String ID IP Address  Prefix  Rule  Type  CPS-Received  CPS-Limit  Uplink-
Received  Uplink-Limit  Downlink-Received  Downlink-Limit  Total-Received
Total-Limit  Cumulative Dropped Packets
-------------------------------------------------------------------------
-------------------------------------------------------------------------
-----------
   47.27.10.10  32      1     PPS   0             0             0
     0              0                        100                  0
      0               424
Total Rate Limit Entries Shown:1
```

The following table provides the field descriptions:

Field	Description
String ID	The string value.
IP Address	The IP address of the subscriber.
Prefix	The prefix configured for the specified subscriber IP address or subnet.
Rule	The name of the firewall rule.
Type	The type of the rate limit. It can have one of the following values: • Packets Per Second (PPS) • Bits Per Second (BPS) • Connections Per Second (CPS)
CPS-Received	The number of CPS for the subscriber IP address.
CPS-Limit	The configured CPS limit.
Uplink-Received	The uplink traffic (PPS or throughput) received from a subscriber IP or a subnet.
Uplink-Limit	The configured uplink limit (for PPS or throughput).
Downlink-Received	The downlink traffic (PPS or throughput) received from a subscriber IP or a subnet.
Downlink-	The configured downlink limit (for PPS or

Field	Description
Limit	throughput).
Total-Received	The total number of packets received from a subscriber IP or a subnet.
Total-Limit	The configured total limit (for PPS or throughput).
Cumulative Dropped Packets	The total number of packets dropped per second. This count is obtained by adding the dropped packet of the current second to the dropped packets of the previous seconds.

Example

```
ACOS(config)#show fw rate-limit summary
Total memory reserved
        : 1248043008 bytes
Total memory used
        : 4194524 bytes
Number of rate-limit allocation failures
        : 0
Total number of rate-limit entries
        : 0
Total number of rate-limit entries allocated
        : 17
Total number of rate-limit entries freed
        : 17
Number of rate-limit entries with scope Aggregate
        : 0
Number of rate-limit entries with scope Subscriber-IP
        : 0
Number of rate-limit entries with scope Subscriber-Prefix
        : 0
The total number of rate-limiting entries with the scope RADIUS user
group.        : 0
The total number of rate-limiting entries with the scope RADIUS user ID.
        : 0
Number of parent rate-limit entries with scope Aggregate
        : 0
```

```
Number of parent rate-limit entries with scope Subscriber-IP
        : 0
Number of parent rate-limit entries with scope Subscriber-Prefix
        : 0
The total number of parent rate-limiting entries with the scope RADIUS
user group. : 0
The total number of parent rate-limiting entries with the scope RADIUS
user ID.    : 0
```

The following table provides the field descriptions:

Field	Description
Total memory reserved	The total memory reserved for rate-limiting
Total memory used	The memory used during rate-limiting
Number of rate-limit allocation failures	The number of failed rate-limit entries if memory allocation fails
Total number of rate-limit entries	The total number of rate-limit entries
Number of rate-limit entries with scope Aggregate	The number of rate-limit entries with scope Aggregate
Number of rate-limit entries with scope Subscriber-IP	The number of rate-limit entries with scope Subscriber-IP
Number of rate-limit entries with scope Subscriber-Prefix	The number of rate-limit entries with scope Subscriber-Prefix
The total number of rate-limiting entries with the scope RADIUS user group	The total number of rate-limiting entries with the scope RADIUS user group
The total number of rate-limiting entries with the scope RADIUS user ID	The total number of rate-limiting entries with the scope RADIUS user ID
Number of parent rate-limit entries with scope Aggregate	The number of parent rate-limit entries in the template limit policy
Number of parent rate-limit entries with scope Subscriber-IP	The number of parent rate-limit entries with scope Subscriber-IP
Number of parent rate-limit entries with scope Subscriber-Prefix	The number of parent rate-limit entries with scope Subscriber-Prefix

Field	Description
The total number of parent rate-limiting entries with the scope RADIUS user group	The total number of parent rate-limiting entries with the scope RADIUS user group
The total number of parent rate-limiting entries with the scope RADIUS user ID	The total number of parent rate-limiting entries with the scope RADIUS user ID

show fw resource-usage

Description Displays statistics related to resource usage of firewall components and their maximum limits.

Syntax

```
show fw resource-usage [ clause-per-obj-grp | helper-sessions | ip-range | object | object-group | radius-table-size | rule| rule-set | zone]
```

Paremeters	Description
`clause-per-obj-grp`	Display the number of clauses per object group.
`helper-sessions`	Display the statistics of the helper sessions used by the firewall. It also provides information on the number of helper SMP sessions created and the maximum limit of the SMP sessions.
`ip-range`	Display the utilization of IP ranges in the firewall configurations. This provides an insight into how IP address blocks are used in the firewall rules.
`object`	Display the resource usage information for firewall objects.
`object-group`	Display the resource usage information for firewall object-groups.

Paremeters	Description
radius-table-size	Display the size of the RADIUS (Remote Authentication Dial-In User Service) table.
rule	Display resource usage statistics for the firewall rules.
rule-set	Display resource usage statistics for the firewall rule-sets.
zone	Display resource usage statistics for the zones.

Mode All

Example The following example shows sample output for the **show fw resource-usage** command:

```
ACOS(config)# show fw resource-usage
Resource             Current-Used   Total
-------------------------------------------------
object               0              10000
object-group         0              1000
rule-set             4              256
rule                 4              8000
zone                 0              256
ip-range             0              256
helper-sessions      0              524288
radius-table-size    0              4000000
clause-per-obj-grp   N/A            64
```

Example The following example shows sample output for the **show fw resource-usage** command on a Multi-PU platform:

```
Master
Resource             Current-Used   Total
-------------------------------------------------
object               0              256000
object-group         0              8000
rule-set             0              4096
rule                 0              256000
```

```
zone                  0               4096
ip-range              0               4096
helper-sessions       0               67108863

Blade: 1
Resource              Current-Used    Total
-------------------------------------------------
object                0               256000
object-group          0               8000
rule-set              0               4096
rule                  0               256000
zone                  0               4096
ip-range              0               4096
helper-sessions       0               67108863
```

show fw server

Description View Firewall real server information.

Syntax

```
show fw server server-name
```

Mode All

Example The following example shows sample output for the **show fw server** command:

```
ACOS (config)#show fw server
Total Number of Servers configured: 1
Total Number of Services configured: 1
                    Current = Current Connections, Total =
Total Connections
                    Fwd-pkt = Forward packets, Rev-pkt =
Reverse packets
Service                     Current    Total      Fwd-pkt
Rev-pkt    Peak-conn  State
-------------------------------------------------------------
-------------------------
s1:514/udp                  0          0          692        0
       0          Up
```

```
s1: Total                  0          0          692        0
       0          Up
```

show fw service-group

Description display the status and statistics for a specific firewall service group.

Syntax **show fw service-group** *service-group-name*

Mode All

Example The following example shows sample output for the **show fw service-group** command:

```
ACOS (config-if:ethernet:2)#show fw service-group fw_sg1
Service group name: fw_sg1
State:                            All Up
Service selection fail drop:      0
Service selection fail reset:     0
Service peak connection:          0
Service: fw_server1:514           UP
Forward packets:                  0
Reverse packets:                  0
Forward bytes:                    0
Reverse bytes:                    0
Current connections:              0
Persistent connections:           0
Current requests:                 0
Total requests:                   0
Total connections:                0
Response time:                    0 (usec)
Fastest Rsp time:                 0
Slowest Rsp time:                 0 (10usec)
Total requests succ:              0
Peak conn:                        0
```

Field	Description
Service group name	The name of the service group.

Field	Description
State	The state of the service group.
Service selection fail drop	The number of times packets were dropped because the firewall service-group failed to select a service.
Service selection fail reset	The number of times connections were reset because the firewall service-group failed to select a service.
Service peak connection	The maximum number of simultaneous connections to the firewall service group.
Service	Indicates the server name, port and status.
Forward packets	The number of packets forwarded to the server.
Reverse packets	The number of packets received from the server.
Forward bytes	The total bytes forwarded to the server.
Reverse bytes	The total bytes received from the server.
Current connections	The current number of active connections to the server.
Persistent connections	The number of persistent connections to the server.
Current requests	The number of current requests being processed by the server.
Total requests	The total number of requests processed by the server.
Total connections	The total number of connections established to the server.
Response time	The average response time from the

Field	Description
	server in microseconds.
Fastest Rsp time	The fastest response time from the server.
Slowest Rsp time	The slowest response time from the server.
Total requests succ	The total number of successful requests processed by the server.
Peak conn	The peak number of simultaneous connections to the server.

show fw status

Description View Firewall rule-set compilation status.

Syntax

```
show fw status [internal]
```

Parameter	Description
internal	For use by A10 Networks Technical Support.

Mode All

Example The following example shows sample output for the **show fw status** command:

```
ACOS# show fw status
Current Active Rule-set                    :      ruleset2
Previous Successful Compilation Attempt    :      2016-03-11
06:59:39
Previous Successful Compilation Duration   :      Less than a
millisecond
Most Recent Compilation Attempt            :      2016-03-20
06:59:39
Most Recent Compilation Status             :      Successful
```

Example The following example shows sample output for the **show fw status** command on a Multi-PU platform:

```
PU: 1
Current Active Rule-set                    :      ruleset1
Previous Successful Compilation Attempt    :      2025-10-14
19:33:19
Previous Successful Compilation Duration   :      8 milliseconds
Most Recent Compilation Attempt            :      2025-10-14
19:33:19
Most Recent Compilation Status             :      Successful

PU: 2
Current Active Rule-set                    :      ruleset1
Previous Successful Compilation Attempt    :      2025-10-14
19:33:19
Previous Successful Compilation Duration   :      Less than a
millisecond
Most Recent Compilation Attempt            :      2025-10-14
19:33:19
Most Recent Compilation Status             :      Successful
```

The following table describes the fields in the output above:

Field	Description
Current Active Rule-set	Name of the currently active rule-set.
Previous Successful Compilation Attempt	Timestamp for the last successful compilation of this rule-set, for example, the previous time the rules in the rule-set were rearranged.
Previous Successful Compilation Duration	Time required for the rule-set compilation to complete.
Most Recent Compilation Attempt	Timestamp (date and time) when this rule-set compilation was attempted.
Most Recent	Status of most recent rule-set compilation:

Field	Description
Compilation Status	• In Progress • Success • Failed

show fw system-status

Description View the Firewall system status information for CPU usage, memory usage, sessions used, and RADIUS table metrics.

Syntax

```
show fw system-status
```

Mode All

Example The following example shows sample output for the **show fw system-status** command:

```
AX5100#show fw system-status
CPU Usage:
----------
Control CPU 1 :  15%
Data CPU 1    :   0%
Data CPU 2    :   0%
Data CPU 3    :   0%
Data CPU 4    :   0%
Data CPU 5    :   0%
Data CPU 6    :   0%
Data CPU 7    :   0%
Data CPU 8    :   0%
Data CPU 9    :   0%
Data CPU 10   :   0%
Data CPU 11   :   0%
Data CPU 12   :   0%
Data CPU 13   :   0%
Data CPU 14   :   0%
Data CPU 15   :   0%
Data CPU avg  :   0%

Memory Status:
```

```
--------------
Total Memory(KB): 24674588
Used Memory(KB) : 16727080
Free Memory(KB) : 7947508
Memory Usage    : 67.7%

Sessions Status:
----------------
Data Sessions Used: 0
Data Sessions Free: 67010545
SMP Sessions Used : 0
SMP Sessions Free : 66519040

RADIUS Table Usage:
-------------------
RADIUS Entries Used: 0
RADIUS Entries Free: 6000000
```

Example The following example shows sample output for the **show fw system-status** command on a Multi-PU platform:

```
Master:
CPU Usage:
----------
Control CPU 1 : 28%
Control CPU 2 : 13%

Data CPU 1    :   0%
Data CPU 2    :   0%
Data CPU 3    :   0%
Data CPU 4    :   0%
Data CPU 5    :   0%
Data CPU 6    :   0%
Data CPU 7    :   0%
Data CPU 8    :   0%
Data CPU 9    :   0%
Data CPU 10   :   0%
Data CPU 11   :   0%
Data CPU 12   :   0%
Data CPU 13   :   0%
Data CPU 14   :   0%
```

```
Data CPU 15    :    0%

Memory Status:
--------------
Total Memory(KB): 262196564
Used Memory(KB) : 31877804
Free Memory(KB) : 230318760
Memory Usage    : 12.1%

Sessions Status:
----------------
Data Sessions Used: 0
Data Sessions Free: 268009378
SMP Sessions Used : 0
SMP Sessions Free : 265748475

RADIUS Table Usage:
-------------------
RADIUS Entries Used: 0
RADIUS Entries Free: 32000000

Blade 1:
CPU Usage:
----------
Control CPU 1 : 8%
Control CPU 2 : 25%

Data CPU 1     :    0%
Data CPU 2     :    0%
Data CPU 3     :    0%
Data CPU 4     :    0%
Data CPU 5     :    0%
Data CPU 6     :    0%
Data CPU 7     :    0%
Data CPU 8     :    0%
Data CPU 9     :    0%
Data CPU 10    :    0%
Data CPU 11    :    0%
Data CPU 12    :    0%
Data CPU 13    :    0%
```

```
Data CPU 14    :    0%
Data CPU 15    :    0%

Memory Status:
--------------
Total Memory(KB): 262196564
Used Memory(KB) : 31444632
Free Memory(KB) : 230761932
Memory Usage    : 11.9%

Sessions Status:
----------------
Data Sessions Used: 0
Data Sessions Free: 268009401
SMP Sessions Used : 0
SMP Sessions Free : 265748475

RADIUS Table Usage:
-------------------
RADIUS Entries Used: 0
RADIUS Entries Free: 32000000
```

show fw tcp syn-cookie statistics

Description View statistics related to TCP SYN cookies.

Syntax

```
show fw tcp syn-cookie statistics
```

Mode All

Example The following example shows sample output for **show fw tcp syn-cookie statistics** command:

```
ACOS (config)# show fw tcp syn-cookie statistics
TCP SYN cookie protection on                                0
TCP SYN cookie SYN ACK Sent                                 0
TCP SYN cookie verification passed                          0
TCP SYN cookie verification failed                          0
```

Field	Description
TCP SYN cookie protection on	Determines if syn-cookie protection is enabled. 1 indicates that protection is on. 0 indicates syn-cookie protection is off.
TCP SYN cookie SYN ACK Sent	The number of TCP SYN ACK packets sent by the device using TCP SYN cookies.
TCP SYN cookie verification passed	The number of times TCP SYN cookie verification process succeeds.
TCP SYN cookie verification failed	The number of times the TCP SYN cookie verification process fails.

show fw top-k-rules

Description View the statistics related to the most frequently matched firewall rules.

Syntax

```
clear fw top-k-rules metric-name { Permit-Rules | Deny-Rules | Reset-Rules }
```

Parameter	Description
metric-name	Specify the metric for which the firewall rules statistics need to be displayed.
You can specify one of the following options:	
Permit-Rules	Display the statistics for the top rules that permit the traffic.
Deny-Rules	Display the statistics for the top rules that deny the traffic.
Reset-Rules	Display the statistics for the top rules that reset the connection or session.

Mode All

Usage Use this command to optimize and refine the firewall rule-set. This command allows you to focus on rules that are being used actively and also helps in identifying and revising rules that do not serve the purpose.

show local-log database all/stats/file

Description For application aware firewall, this command provides basic log storage, basic filtered log search and retrieval, and top N analysis based on log content for application aware firewall.

Syntax `show local-log database {all | stats | name <1-127>}`

Parameter	Description
all	List all databases
stats	Show the statistics of local-log databases
name 1-127	Show the information of a specific database

Mode All

Example

```
ACOS(config:1)# show local-log database all
Database name
 Size
------------------------------------------------------------------
-------------------------
app_fw_app_top_src_l1_20171207124800
 6.1 KBytes
app_fw_app_top_src_l2_20171207130000
 6.1 KBytes
app_fw_log_20171206044838
 11.2 KBytes
app_fw_top_app_l1_20171207124800
 5.1 KBytes
app_fw_top_app_l2_20171207130000
 5.1 KBytes
```

```
app_fw_top_category_l1_20171207124800
 10.2 KBytes
app_fw_top_category_l2_20171207130000
 10.2 KBytes
app_fw_top_src_l1_20171207124800
 5.1 KBytes
app_fw_top_src_l2_20171207130000
 5.1 KBytes
local_log_mapping
 29.6 KBytes
local_log_mgr
 11.2 Kbytes
```

```
ACOS(config:1)# show local-log database stats
Harddisk space occupied:                105.4 KBytes
Auth-log database number:               0
Auth-log database total size:           0 Bytes
Auth-log record number:                 0
Access-log database number:             0
Access-log database total size:         0 Bytes
Access-log record number:               0
File-Category database number:          0
File-Category database total size:      0 Bytes
File-Category record number:            0
App-Firewall database number:           9
App-Firewall database total size:       64.5 KBytes
App-Firewall record number:             56

ACOS(config)# show local-log database app_fw_log_
20171206044838
Database type:                          Application Firewall
[raw]
Size:                                   11.2 KBytes
Record number:                          56
Start time:                             12:43:16 12/07/2017
End time:                               12:49:22 12/07/2017
```

show rule-set

Description View Firewall information for a rule-set.

Syntax

```
show rule-set name
[rules-by-zone]
    [from zone-name]
    [tozone-name]
]
```

Parameter	Description
rules-by-zone	View statistics for a rule-set based on zone. all traffic-maps, or view a traffic-map for a specific service *name*.
from *zone-name*	Name of the zone from which traffic is coming.
to *zone-name*	Name of the zone to which traffic is going.

Mode All

Example The following example shows sample output for the **show rule-set** command:

```
AX2500(config)#show rule-set rs1
Rule-Set-Name: rs1
Rule-Set-Status: active
Unmatched-Drops: 0    Action-Permit: 3    Action-Deny: 0
Action-Reset: 0
Total-Rule-Count: 3

Rule-Name:                      rule1
Hit-Count:                      3
Action:                         permit
Status:                         enable
Permit-bytes:                   214
Deny-bytes:                     0
Reset-bytes:                    0
Total-bytes:                    214
Permit-packets:                 0
```

```
Deny-packets:                    0
Reset-packets:                   0
Total-packets:                   0
TCP-active-session:              0
UDP-active-session:              0
ICMP-active-session:             0
SCTP-active-session:             1
OTHER-protocol-active-session:   0
Total-active-session:            1
TCP-session:                     0
UDP-session:                     0
ICMP-session:                    0
SCTP-session:                    1
OTHER-protocol-session:          0
Total-session:                   1
Rate-limit-drops:                0
----TCP SYN cookie----
protection on:                   0
Syn-Ack-Sent:                    0
Verification-Passed:             0
Verification-Failed:             0
Tcp-Half-Open-Count:             0
```

show rule-set (application firewall)

Description For Application Firewall, displays the rule-set statistics for an application, protocol or category.

Syntax

```
show rule-set <rule-set name> application [category |
{protocol [in-category]}]
```

Mode All

Usage This command is used to view the statistics of the rule-set for an application by category or protocol. For dual blade Multi-PU platforms, the statistics will display the aggregated counters of PU1 and PU2 (PU1 + PU2).

Example

```
1. AX1030(config)# show rule-set rs application category
```

```
 Rule name          App/Category
  Conns     Bytes
 ------------------------------------------------------------
------
 Rule-set: rs
                    basic
  18         15691844
                    networking
  2180       519937
                    instant-messaging-and-multimedia-
conferencing 45         839759
                    chat
  44         815176
                    file-transfer
  1          24583
                    social-networks
  59         2817009
                    voip
  1          24583
                    web
  757        35396442
                    web-search-engines
  5          37022
                    web-e-commerce
  9          69835
                    web-websites
  19         198226
                    mobile
  310        13132872
                    file-management
  2          4094
                    enterprise
  62         256354
                    software-update
  2          9112
                    aaa
  15         54959
                    remote-access
  59         248642
```

```
                    multimedia-streaming
 272        10953648
                    cdn
 16         591818
                    advertising
 220        2368405
                    analytics-and-statistics
 69         1704177
                    standards-based
 2213       16266740
                    cloud-based-services
 4          558997
Rule: 1
                    basic
 18         15691844
                    networking
 2180       519937
                    instant-messaging-and-multimedia-
conferencing 45         839759
                    chat
 44         815176
                    file-transfer
 1          24583
                    social-networks
 59         2817009
                    voip
 1          24583
                    web
 757        35396442
                    web-search-engines
 5          37022
                    web-e-commerce
 9          69835
                    web-websites
 19         198226
                    mobile
 310        13132872
                    enterprise
 48         251902
```

```
                    software-update
  2          9112
                    aaa
  15         54959
                    remote-access
  45         244190
                    multimedia-streaming
  272        10953648
                    cdn
  16         591818
                    advertising
  220        2368405
                    analytics-and-statistics
  69         1704177
                    standards-based
  2213       16266740
                    cloud-based-services
  4          558997

2. ACOS(config)# show rule-set rs application category rule 1
Rule name          App/Category
 Conns     Bytes
 ------------------------------------------------------------
------
 Rule: 1
                    basic
  18         15691844
                    networking
  2183       520752
                    instant-messaging-and-multimedia-
conferencing 45         839759
                    chat
  44         815176
                    file-transfer
  1          24583
                    social-networks
  59         2817009
                    voip
  1          24583
```

```
                  web
 758        35402321
                  web-search-engines
 5          37022
                  web-e-commerce
 9          69835
                  web-websites
 19         198226
                  mobile
 310        13132992
                  enterprise
 48         251902
                  software-update
 2          9112
                  aaa
 15         54959
                  remote-access
 45         244190
                  multimedia-streaming
 272        10953768
                  cdn
 16         591818
                  advertising
 220        2368405
                  analytics-and-statistics
 69         1704177
                  standards-based
 2216       16267555
                  cloud-based-services
 4          558997

3. ACOS(config)# show rule-set rs application category
multimedia-streaming
 Rule name          App/Category          Conns     Bytes
 ------------------------------------------------------------
 Rule-set: rs
                  multimedia-streaming 274       10957056
 Rule: 1
                  multimedia-streaming 274       10957056
```

```
4. ACOS(config)# show rule-set rs application protocol
 Rule name          App/Category       Conns     Bytes
 ------------------------------------------------------------
 Rule-set: rs
                    addthis            1         1555
                    adobe              2         12193
                    adsafeprotected    19        198226
                    amazon             9         69835
                    amazon_adsystem    14        51193
                    amazon_aws         4         558997
                    apple              14        586453
                    appnexus           31        448538
                    atlassolutions     1         8185
                    bing               5         37022
                    cnn                254       10320826
                    criteo             11        38764
                    dns                2191      522732
                    facebook           44        815176
                    fastly             12        32821
                    google_ads         54        777001
                    google_analytics   1         7755
                    google_gen         31        337162
                    google_tags        12        71714
                    gstatic            8         50773
                    http               9         21968
                    https              9         15669876
                    indexexchange      5         27909
                    krux               10        686620
                    moat               33        622540
                    mozilla            7         41139
                    netflix            19        628364
                    ocsp               15        54959
                    optimizely         16        340531
                    outbrain           44        250987
                    quantcast          8         38546
                    rubiconproject     24        149488
                    sharethrough       16        416559
                    signal             3         24175
                    skype              1         24583
                    smb                2         4094
```

```
                    symantec            3          7712
                    teamviewer          59         248642
                    turner              1          7866
                    twitter             14         2000278
                    windows_update      2          9112
Rule: 1
                    addthis             1          1555
                    adobe               2          12193
                    adsafeprotected     19         198226
                    amazon              9          69835
                    amazon_adsystem     14         51193
                    amazon_aws          4          558997
                    apple               14         586453
                    appnexus            31         448538
                    atlassolutions      1          8185
                    bing                5          37022
                    cnn                 254        10320826
                    criteo              11         38764
                    dns                 2191       522732
                    facebook            44         815176
                    fastly              12         32821
                    google_ads          54         777001
                    google_analytics    1          7755
                    google_gen          31         337162
                    google_tags         12         71714
                    gstatic             8          50773
                    http                9          21968
                    https               9          15669876
                    indexexchange       5          27909
                    krux                10         686620
                    moat                33         622540
                    mozilla             7          41139
                    netflix             19         628364
                    ocsp                15         54959
                    optimizely          16         340531
                    outbrain            44         250987
                    quantcast           8          38546
                    rubiconproject      24         149488
                    sharethrough        16         416559
                    signal              3          24175
```

```
                    skype               1          24583
                    symantec            3          7712
                    teamviewer          45         244190
                    turner              1          7866
                    twitter             14         2000278
                    windows_update      2          9112

5. ACOS(config)# show rule-set rs application protocol
facebook
 Rule name          App/Category       Conns      Bytes
 ------------------------------------------------------
 Rule-set: rs
                    facebook           44         815176
 Rule: 1
                    facebook           44         815176

6. ACOS(config)# show rule-set rs application protocol in-
category social-networks
 Rule name          App/Category       Conns      Bytes
 ------------------------------------------------------
 Rule-set: rs
                    addthis            1          1555
                    facebook           44         815176
                    twitter            14         2000278
 Rule: 1
                    addthis            1          1555
                    facebook           44         815176
                    twitter            14         2000278
 Rule: rule-1
```

show sctp statistics

Description View SCTP statistics.

Syntax

```
show sctp statistics
```

Mode All

Example The following example shows sample output for the **show sctp statistics** command:

```
ACOS(config)# show sctp statistics
SCTP Statistics:
----------------
SCTP Static NAT Session Created                    0
SCTP Static NAT Session Deleted                    0
SCTP Firewall Session Created                      0
SCTP Firewall Session Deleted                      0
Packet Error Drop                                  0
Out-of-state Packet Drop                           0
Maximum Multi-homing IP Addresses Drop             0
Multi-homing Remove IP Parameter Skip              0
Multi-homing IP Address Not Found Drop             0
Static NAT Config Not Found Drop                   0
Configuration Error Drop                           0
NAT Resource VRRP-A Standby Drop                   0
Invalid Fragmented Chunks Drop                     0
Disallowed Chunk Filtered                          0
Disallowed Packet Drop                             0
Rate-limit Drop                                    0
Standby Session Created                            0
Standby Session Create Failed                      0
Standby Session Updated                            0
Standby Session Update Failed                      0
Static NAT Config Not Found on Standby             0
```

show session application

Description For application aware firewall, displays classified session entries.

Syntax

```
show session application {category | protocol} <name>
```

Mode All

Usage Used to view the classified session information for a category or protocol.

Example

```
1.ACOS(config)#show session application
Traffic Type                          Total
-------------------------------------------
```

```
Total Sessions                      555
TCP Established                     119
TCP Half Open                       436
SCTP Established                    0
SCTP Half Open                      0
UDP                                 0
Non TCP/UDP IP sessions             0
Other                               1
Reverse NAT TCP                     555
Reverse NAT UDP                     0
Curr Free Conn                      16784242
Conn Count                          205839
Conn Freed                          204724
TCP SYN Half Open                   0
Conn SMP Alloc                      45
Conn SMP Free                       21
Conn SMP Aged                       15
Conn Type 0 Available               32374774
Conn Type 1 Available               16350650
Conn Type 2 Available               8093134
Conn Type 3 Available               4005888
Conn Type 4 Available               2002944
Conn SMP Type 0 Available           32047104
Conn SMP Type 1 Available           16023552
Conn SMP Type 2 Available           8028156
Conn SMP Type 3 Available           4014072
Conn SMP Type 4 Available           2002944
Total Local Sessions                1
Prot Forward Source             Forward Dest
Reverse Source             Reverse Dest              Age   Hash
Flags    Type     Application
-------------------------------------------------------------
-----
Tcp  172.16.1.67:53362          172.217.24.6:443
172.217.24.6:443           192.168.91.24:3372        300   1
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52377          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3322        300   1
NFe0f0r0 NAT      amazon
```

```
Tcp  172.16.1.67:52192          52.89.245.86:443
52.89.245.86:443          192.168.91.24:3312        300   1
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52472          23.48.132.80:443
23.48.132.80:443          192.168.91.24:3327        300   1
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52787          31.13.87.5:443
31.13.87.5:443            192.168.91.24:3347        300   1
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52127          104.88.153.161:443
104.88.153.161:443        192.168.91.24:3297        300   1
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:53232          172.217.160.66:443
172.217.160.66:443        192.168.91.24:3367        300   1
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52652          13.228.215.38:443
13.228.215.38:443         192.168.91.24:3332        300   1
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:53907          54.239.29.0:443
54.239.29.0:443           192.168.91.24:3377        300   1
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52172          54.230.214.164:443
54.230.214.164:443        192.168.91.24:3302        300   1
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52662          192.229.237.96:443
192.229.237.96:443        192.168.91.24:3337        300   1
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:53222          172.217.24.14:443
172.217.24.14:443         192.168.91.24:3362        300   1
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:52177          104.115.248.121:443
104.115.248.121:443       192.168.91.24:3307        300   1
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52887          172.217.27.131:443
172.217.27.131:443        192.168.91.24:3352        300   1
NFe0f0r0 NAT      gstatic
Tcp  172.16.1.67:52057          54.230.214.164:443
54.230.214.164:443        192.168.91.24:3287        300   1
NFe0f0r0 NAT      amazon
```

```
Tcp  172.16.1.67:52122          104.88.153.161:443
104.88.153.161:443        192.168.91.24:3292        300   1
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:53217          104.115.248.121:443
104.115.248.121:443       192.168.91.24:3357        300   1
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52252          54.230.214.164:443
54.230.214.164:443        192.168.91.24:3317        300   1
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52667          192.229.237.96:443
192.229.237.96:443        192.168.91.24:3342        300   1
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:53228          52.41.20.47:443
52.41.20.47:443           192.168.91.24:3368        300   2
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52708          117.18.237.70:443
117.18.237.70:443         192.168.91.24:3348        300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52173          54.230.214.164:443
54.230.214.164:443        192.168.91.24:3293        300   2
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:53233          172.217.160.66:443
172.217.160.66:443        192.168.91.24:3373        300   2
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52058          104.115.248.121:443
104.115.248.121:443       192.168.91.24:3283        300   2
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52178          104.115.248.121:443
104.115.248.121:443       192.168.91.24:3298        300   2
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52473          23.48.132.80:443
23.48.132.80:443          192.168.91.24:3328        300   2
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52123          104.88.153.161:443
104.88.153.161:443        192.168.91.24:3288        300   2
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52378          54.230.214.164:443
54.230.214.164:443        192.168.91.24:3318        300   2
NFe0f0r0 NAT      amazon
```

```
Tcp  172.16.1.67:53226          216.58.200.238:80
216.58.200.238:80          192.168.91.24:50956        300   2
NFe0f0r0 NAT      ocsp
Tcp  172.16.1.67:52253          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3313         300   2
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52783          34.197.194.240:443
34.197.194.240:443         192.168.91.24:3358         300   2
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:53363          172.217.24.6:443
172.217.24.6:443           192.168.91.24:3378         300   2
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52538          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3333         300   2
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:53698          172.217.160.78:443
172.217.160.78:443         192.168.91.24:3388         300   2
NFe0f0r0 NAT      google_analytics
Tcp  172.16.1.67:53223          52.84.202.194:443
52.84.202.194:443          192.168.91.24:3363         300   2
NFe0f0r0 NAT      mozilla
Tcp  172.16.1.67:53683          104.244.42.72:443
104.244.42.72:443          192.168.91.24:3383         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52663          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3343         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52658          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3338         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52193          52.89.245.86:443
52.89.245.86:443           192.168.91.24:3308         300   2
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52423          74.125.204.94:443
74.125.204.94:443          192.168.91.24:3323         300   2
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:52183          104.244.42.1:443
104.244.42.1:443           192.168.91.24:3303         300   2
NFe0f0r0 NAT      twitter
```

```
Tcp  172.16.1.67:53234          52.193.134.160:443
52.193.134.160:443         192.168.91.24:3154         300   3
NFe0f0r0 NAT      signal
Tcp  172.16.1.67:52379          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3109         300   3
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52429          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3114         300   3
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52189          52.89.245.86:443
52.89.245.86:443           192.168.91.24:3094         300   3
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52022          23.41.139.27:80
23.41.139.27:80            192.168.91.24:51037        300   3
NFe0f0r0 NAT      ocsp
Tcp  172.16.1.67:53349          72.21.206.140:443
72.21.206.140:443          192.168.91.24:3159         300   3
NFe0f0r0 NAT      amazon_adsystem
Tcp  172.16.1.67:51944          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3074         300   3
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52474          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3119         300   3
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52254          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3104         300   3
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:53364          52.89.83.216:443
52.89.83.216:443           192.168.91.24:3164         300   3
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52184          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3089         300   3
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52234          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3099         300   3
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52664          192.229.237.96:443
192.229.237.96:443         192.168.91.24:3134         300   3
NFe0f0r0 NAT      twitter
```

```
Tcp  172.16.1.67:52709          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3139         300   3
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52659          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3129         300   3
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52959          31.13.87.8:443
31.13.87.8:443             192.168.91.24:3144         300   3
NFe0f0r0 NAT      atlassolutions
Tcp  172.16.1.67:52179          104.115.248.121:443
104.115.248.121:443        192.168.91.24:3084         300   3
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52124          104.88.153.161:443
104.88.153.161:443         192.168.91.24:3079         300   3
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:53340          172.217.160.98:443
172.217.160.98:443         192.168.91.24:3490         300   4
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:53230          216.58.200.226:443
216.58.200.226:443         192.168.91.24:3485         300   4
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52665          192.229.237.96:443
192.229.237.96:443         192.168.91.24:3475         300   4
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52190          52.89.245.86:443
52.89.245.86:443           192.168.91.24:3440         300   4
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52375          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3455         300   4
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52125          104.88.153.161:443
104.88.153.161:443         192.168.91.24:3430         300   4
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52710          74.125.204.94:443
74.125.204.94:443          192.168.91.24:3480         300   4
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:53365          216.58.200.38:443
216.58.200.38:443          192.168.91.24:3500         300   4
NFe0f0r0 NAT      google_ads
```

```
Tcp  172.16.1.67:53570          104.244.42.67:443
104.244.42.67:443          192.168.91.24:3505         300   4
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52660          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3470         300   4
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:51945          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3425         300   4
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:58803          217.146.31.4:80
217.146.31.4:80            192.168.91.24:41583        300   4
NFe0f0r0 NAT      teamviewer
Tcp  172.16.1.67:52255          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3450         300   4
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:51825          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3410         300   4
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52180          104.115.248.121:443
104.115.248.121:443        192.168.91.24:3435         300   4
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52235          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3445         300   4
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52470          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3460         300   4
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:51895          34.197.194.240:443
34.197.194.240:443         192.168.91.24:3420         300   4
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:53345          74.125.204.147:443
74.125.204.147:443         192.168.91.24:3495         300   4
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:58864          217.146.31.4:80
217.146.31.4:80            192.168.91.24:42209        300   5
NFe0f0r0 NAT      teamviewer
Tcp  172.16.1.67:53231          172.217.160.66:443
172.217.160.66:443         192.168.91.24:3451         300   5
NFe0f0r0 NAT      google_ads
```

```
Tcp  172.16.1.67:52376          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3406         300    5
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52171          54.230.214.164:443
54.230.214.164:443         192.168.91.24:3391         300    5
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52661          192.229.237.96:443
192.229.237.96:443         192.168.91.24:3416         300    5
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52021          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3376         300    5
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52746          172.217.27.131:443
172.217.27.131:443         192.168.91.24:3431         300    5
NFe0f0r0 NAT      gstatic
Tcp  172.16.1.67:51896          54.192.212.211:443
54.192.212.211:443         192.168.91.24:3366         300    5
NFe0f0r0 NAT      amazon
Tcp  172.16.1.67:52191          52.89.245.86:443
52.89.245.86:443           192.168.91.24:3401         300    5
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:52176          104.115.248.121:443
104.115.248.121:443        192.168.91.24:3396         300    5
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:51951          52.26.219.81:443
52.26.219.81:443           192.168.91.24:3371         300    5
NFe0f0r0 NAT      netflix
Tcp  172.16.1.67:53686          104.244.42.65:443
104.244.42.65:443          192.168.91.24:3456         300    5
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:53001          74.125.204.147:443
74.125.204.147:443         192.168.91.24:3441         300    5
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:52126          104.88.153.161:443
104.88.153.161:443         192.168.91.24:3386         300    5
NFe0f0r0 NAT      apple
Tcp  172.16.1.67:52471          23.48.132.80:443
23.48.132.80:443           192.168.91.24:3411         300    5
NFe0f0r0 NAT      netflix
```

```
Tcp  172.16.1.67:52786          216.58.200.234:443
216.58.200.234:443        192.168.91.24:3436        300   5
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:52666          192.229.237.96:443
192.229.237.96:443        192.168.91.24:3421        300   5
NFe0f0r0 NAT      twitter

2. ACOS(config)#show session application protocol facebook
Traffic Type                          Total
-------------------------------------------
Total Sessions                        515
TCP Established                       111
TCP Half Open                         404
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               0
Other                                 1
Reverse NAT TCP                       515
Reverse NAT UDP                       0
Curr Free Conn                        16784326
Conn Count                            209991
Conn Freed                            208960
TCP SYN Half Open                     0
Conn SMP Alloc                        54
Conn SMP Free                         30
Conn SMP Aged                         24
Conn Type 0 Available                 32374774
Conn Type 1 Available                 16350692
Conn Type 2 Available                 8093176
Conn Type 3 Available                 4005888
Conn Type 4 Available                 2002944
Conn SMP Type 0 Available             32047104
Conn SMP Type 1 Available             16023552
Conn SMP Type 2 Available             8028156
Conn SMP Type 3 Available             4014072
Conn SMP Type 4 Available             2002944
Total Local Sessions                  1
```

```
Prot Forward Source            Forward Dest
Reverse Source            Reverse Dest               Age   Hash
Flags    Type     Application
-------------------------------------------------------------
-
Tcp  172.16.1.67:52787         31.13.87.5:443
31.13.87.5:443            192.168.91.24:3347         300   1
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52538         31.13.87.36:443
31.13.87.36:443           192.168.91.24:3333         300   2
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52184         31.13.87.36:443
31.13.87.36:443           192.168.91.24:3089         300   3
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:51825         31.13.87.36:443
31.13.87.36:443           192.168.91.24:3410         300   4
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52021         31.13.87.36:443
31.13.87.36:443           192.168.91.24:3376         300   5
NFe0f0r0 NAT      facebook

3.ACOS(config)#show session application category social-
networks
Traffic Type                          Total
-------------------------------------------
Total Sessions                        531
TCP Established                       103
TCP Half Open                         428
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               0
Other                                 2
Reverse NAT TCP                       531
Reverse NAT UDP                       0
Curr Free Conn                        16784292
Conn Count                            210740
Conn Freed                            209676
TCP SYN Half Open                     0
Conn SMP Alloc                        56
```

```
Conn SMP Free                          31
Conn SMP Aged                          25
Conn Type 0 Available                  32374774
Conn Type 1 Available                  16350674
Conn Type 2 Available                  8093160
Conn Type 3 Available                  4005888
Conn Type 4 Available                  2002944
Conn SMP Type 0 Available              32047104
Conn SMP Type 1 Available              16023552
Conn SMP Type 2 Available              8028156
Conn SMP Type 3 Available              4014072
Conn SMP Type 4 Available              2002944
Total Local Sessions                   2
Prot Forward Source            Forward Dest
Reverse Source             Reverse Dest               Age   Hash
Flags    Type     Application
-------------------------------------------------------------------
-----
Tcp  172.16.1.67:52787         31.13.87.5:443
31.13.87.5:443             192.168.91.24:3347         300   1
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52662         192.229.237.96:443
192.229.237.96:443         192.168.91.24:3337         300   1
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52667         192.229.237.96:443
192.229.237.96:443         192.168.91.24:3342         300   1
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52708         117.18.237.70:443
117.18.237.70:443          192.168.91.24:3348         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52538         31.13.87.36:443
31.13.87.36:443            192.168.91.24:3333         300   2
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:53683         104.244.42.72:443
104.244.42.72:443          192.168.91.24:3383         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52663         117.18.237.70:443
117.18.237.70:443          192.168.91.24:3343         300   2
NFe0f0r0 NAT      twitter
```

```
Tcp  172.16.1.67:52658          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3338         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52183          104.244.42.1:443
104.244.42.1:443           192.168.91.24:3303         300   2
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52184          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3089         300   3
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52664          192.229.237.96:443
192.229.237.96:443         192.168.91.24:3134         300   3
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52709          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3139         300   3
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52659          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3129         300   3
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52665          192.229.237.96:443
192.229.237.96:443         192.168.91.24:3475         300   4
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:53570          104.244.42.67:443
104.244.42.67:443          192.168.91.24:3505         300   4
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52660          117.18.237.70:443
117.18.237.70:443          192.168.91.24:3470         300   4
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:51825          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3410         300   4
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52661          192.229.237.96:443
192.229.237.96:443         192.168.91.24:3416         300   5
NFe0f0r0 NAT      twitter
Tcp  172.16.1.67:52021          31.13.87.36:443
31.13.87.36:443            192.168.91.24:3376         300   5
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:53686          104.244.42.65:443
104.244.42.65:443          192.168.91.24:3456         300   5
NFe0f0r0 NAT      twitter
```

```
Tcp  172.16.1.67:52666          192.229.237.96:443
192.229.237.96:443        192.168.91.24:3421        300    5
NFe0f0r0 NAT      twitter
```

show session filter

Description For application aware firewall, displays the filter session information

Syntax

```
show session filter filter-name
```

Mode All

Usage Used to view the filter session information for an application

Example

```
ACOS(config)#show session filter web
/axapi/v3/sessions/oper?filter_type=filter&name-str=web
raffic Type                          Total
-------------------------------------------
Total Sessions                        663
TCP Established                       110
TCP Half Open                         553
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               0
Other                                 3
Reverse NAT TCP                       663
Reverse NAT UDP                       0
Curr Free Conn                        16783998
Conn Count                            215482
Conn Freed                            214131
TCP SYN Half Open                     0
Conn SMP Alloc                        72
Conn SMP Free                         40
Conn SMP Aged                         34
Conn Type 0 Available                 32374774
Conn Type 1 Available                 16350523
Conn Type 2 Available                 8093017
Conn Type 3 Available                 4005888
```

```
Conn Type 4 Available                2002944
Conn SMP Type 0 Available            32047104
Conn SMP Type 1 Available            16023552
Conn SMP Type 2 Available            8028156
Conn SMP Type 3 Available            4014072
Conn SMP Type 4 Available            2002944
Total Local Sessions                 3
Prot Forward Source             Forward Dest
Reverse Source             Reverse Dest                Age   Hash
Flags    Type     Application
-------------------------------------------------------------------
-----
Tcp  172.16.1.67:52850          104.254.150.4:80
104.254.150.4:80           192.168.91.24:52860         300   1
NFe0f0r0 NAT      appnexus
Tcp  172.16.1.67:52640          23.48.137.41:80
23.48.137.41:80            192.168.91.24:52795         300   1
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52675          151.101.89.67:80
151.101.89.67:80           192.168.91.24:52810         300   1
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52845          172.217.160.66:80
172.217.160.66:80          192.168.91.24:52855         300   1
NFe0f0r0 NAT      google_tags
Tcp  172.16.1.67:52840          151.101.88.249:80
151.101.88.249:80          192.168.91.24:52850         300   1
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53235          54.214.243.98:80
54.214.243.98:80           192.168.91.24:52955         300   1
NFe0f0r0 NAT      krux
Tcp  172.16.1.67:52855          151.101.89.67:80
151.101.89.67:80           192.168.91.24:52865         300   1
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53090          210.176.156.21:80
210.176.156.21:80          192.168.91.24:52910         300   1
NFe0f0r0 NAT      rubiconproject
Tcp  172.16.1.67:52695          54.192.212.223:80
54.192.212.223:80          192.168.91.24:52815         300   1
NFe0f0r0 NAT      sharethrough
```

```
Tcp  172.16.1.67:53195          172.217.160.102:80
172.217.160.102:80         192.168.91.24:52930        300   1
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52970          23.48.137.41:80
23.48.137.41:80            192.168.91.24:52885        300   1
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52655          52.9.29.52:80
52.9.29.52:80              192.168.91.24:52805        300   1
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52830          13.107.21.200:80
13.107.21.200:80           192.168.91.24:52840        300   1
NFe0f0r0 NAT      bing
Tcp  172.16.1.67:53217          31.13.87.5:443
31.13.87.5:443             192.168.91.24:3382         300   1
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:53331          23.53.72.21:80
23.53.72.21:80             192.168.91.24:53171        300   2
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52851          203.69.141.97:80
203.69.141.97:80           192.168.91.24:53091        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53203          31.13.87.5:443
31.13.87.5:443             192.168.91.24:3413         300   2
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52796          23.48.137.41:80
23.48.137.41:80            192.168.91.24:53061        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52683          172.217.160.98:443
172.217.160.98:443         192.168.91.24:3398         300   2
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:52701          203.69.141.27:80
203.69.141.27:80           192.168.91.24:53046        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52656          52.9.29.52:80
52.9.29.52:80              192.168.91.24:53031        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53096          52.197.160.121:80
52.197.160.121:80          192.168.91.24:53136        300   2
NFe0f0r0 NAT      adsafeprotected
```

```
Tcp  172.16.1.67:53091          210.176.156.21:80
210.176.156.21:80          192.168.91.24:53131        300   2
NFe0f0r0 NAT      rubiconproject
Tcp  172.16.1.67:53196          104.115.255.237:80
104.115.255.237:80         192.168.91.24:53146        300   2
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52956          151.101.88.249:80
151.101.88.249:80          192.168.91.24:53106        300   2
NFe0f0r0 NAT      fastly
Tcp  172.16.1.67:52856          151.101.89.67:80
151.101.89.67:80           192.168.91.24:53096        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53206          52.9.29.52:80
52.9.29.52:80              192.168.91.24:53156        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52841          52.84.202.89:80
52.84.202.89:80            192.168.91.24:53081        300   2
NFe0f0r0 NAT      amazon_adsystem
Tcp  172.16.1.67:52846          23.53.72.21:80
23.53.72.21:80             192.168.91.24:53086        300   2
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52703          172.217.17.99:443
172.217.17.99:443          192.168.91.24:3403         0     2
NFe0f0r0 NAT      gstatic
Tcp  172.16.1.67:52696          151.101.89.67:80
151.101.89.67:80           192.168.91.24:53041        300   2
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52933          54.230.214.142:443
54.230.214.142:443         192.168.91.24:3408         300   2
NFe0f0r0 NAT      https
Tcp  172.16.1.67:53201          210.61.248.209:80
210.61.248.209:80          192.168.91.24:53151        300   2
NFe0f0r0 NAT      indexexchange
Tcp  172.16.1.67:52852          151.101.89.67:80
151.101.89.67:80           192.168.91.24:53432        300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53054          172.217.160.98:443
172.217.160.98:443         192.168.91.24:3189         300   3
NFe0f0r0 NAT      google_gen
```

```
Tcp  172.16.1.67:53332          50.31.185.52:80
50.31.185.52:80           192.168.91.24:53512       0     3
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52657          52.9.29.52:80
52.9.29.52:80             192.168.91.24:53362       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53202          52.9.29.52:80
52.9.29.52:80             192.168.91.24:53497       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53372          192.82.211.130:80
192.82.211.130:80         192.168.91.24:53517       0     3
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52694          172.217.17.99:443
172.217.17.99:443         192.168.91.24:3179        300   3
NFe0f0r0 NAT      gstatic
Tcp  172.16.1.67:53087          151.101.88.249:80
151.101.88.249:80         192.168.91.24:53472       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52797          23.48.137.41:80
23.48.137.41:80           192.168.91.24:53402       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52842          104.115.247.69:80
104.115.247.69:80         192.168.91.24:53422       300   3
NFe0f0r0 NAT      rubiconproject
Tcp  172.16.1.67:52697          151.101.89.67:80
151.101.89.67:80          192.168.91.24:53372       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52849          104.115.208.174:443
104.115.208.174:443       192.168.91.24:3184        300   3
NFe0f0r0 NAT      optimizely
Tcp  172.16.1.67:52837          54.192.215.93:80
54.192.215.93:80          192.168.91.24:53417       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52972          23.48.137.41:80
23.48.137.41:80           192.168.91.24:53457       300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52857          151.101.89.67:80
151.101.89.67:80          192.168.91.24:53437       300   3
NFe0f0r0 NAT      cnn
```

```
Tcp  172.16.1.67:53197          151.101.90.2:80
151.101.90.2:80           192.168.91.24:53492        300   3
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52957          151.101.88.249:80
151.101.88.249:80         192.168.91.24:53452        300   3
NFe0f0r0 NAT      fastly
Tcp  172.16.1.67:53199          172.217.27.130:443
172.217.27.130:443        192.168.91.24:3199         300   3
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:53234          31.13.87.36:443
31.13.87.36:443           192.168.91.24:3204         300   3
NFe0f0r0 NAT      facebook
Tcp  172.16.1.67:52682          151.101.89.67:80
151.101.89.67:80          192.168.91.24:53367        300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53097          151.101.89.67:80
151.101.89.67:80          192.168.91.24:53482        300   3
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53099          52.84.203.37:443
52.84.203.37:443          192.168.91.24:3194         300   3
NFe0f0r0 NAT      amazon_aws
Tcp  172.16.1.67:52654          216.58.200.226:443
216.58.200.226:443        192.168.91.24:3174         300   3
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:53092          210.176.156.21:80
210.176.156.21:80         192.168.91.24:53477        300   3
NFe0f0r0 NAT      rubiconproject
Tcp  172.16.1.67:52658          52.9.29.52:80
52.9.29.52:80             192.168.91.24:52838        300   4
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52795          52.71.219.68:443
52.71.219.68:443          192.168.91.24:3510         300   4
NFe0f0r0 NAT      optimizely
Tcp  172.16.1.67:53098          52.94.232.32:80
52.94.232.32:80           192.168.91.24:52938        0     4
NFe0f0r0 NAT      amazon_adsystem
Tcp  172.16.1.67:53093          210.176.156.21:80
210.176.156.21:80         192.168.91.24:52933        300   4
NFe0f0r0 NAT      rubiconproject
```

```
Tcp  172.16.1.67:53460          172.217.27.130:443
172.217.27.130:443         192.168.91.24:3515         300    4
NFe0f0r0 NAT      google_ads
Tcp  172.16.1.67:53198          151.101.90.2:80
151.101.90.2:80            192.168.91.24:52948        300    4
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:53333          50.31.185.52:80
50.31.185.52:80            192.168.91.24:52963        0      4
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:52793          23.48.137.41:80
23.48.137.41:80            192.168.91.24:52868        300    4
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52958          151.101.88.249:80
151.101.88.249:80          192.168.91.24:52903        300    4
NFe0f0r0 NAT      fastly
Tcp  172.16.1.67:52843          54.192.212.135:80
54.192.212.135:80          192.168.91.24:52888        300    4
NFe0f0r0 NAT      adsafeprotected
Tcp  172.16.1.67:52833          151.101.89.67:80
151.101.89.67:80           192.168.91.24:52878        300    4
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52853          151.101.89.67:80
151.101.89.67:80           192.168.91.24:52898        300    4
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53078          18.217.7.76:80
18.217.7.76:80             192.168.91.24:52923        300    4
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52848          182.161.72.67:80
182.161.72.67:80           192.168.91.24:52893        300    4
NFe0f0r0 NAT      criteo
Tcp  172.16.1.67:52698          151.101.89.67:80
151.101.89.67:80           192.168.91.24:52848        300    4
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52684          104.116.19.49:80
104.116.19.49:80           192.168.91.24:53294        300    5
NFe0f0r0 NAT      optimizely
Tcp  172.16.1.67:52844          151.101.88.175:80
151.101.88.175:80          192.168.91.24:53349        300    5
NFe0f0r0 NAT      krux
```

```
Tcp  172.16.1.67:52699          151.101.89.67:80
151.101.89.67:80          192.168.91.24:53299        300    5
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52854          151.101.89.67:80
151.101.89.67:80          192.168.91.24:53354        300    5
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:53094          210.176.156.21:80
210.176.156.21:80         192.168.91.24:53389        300    5
NFe0f0r0 NAT      rubiconproject
Tcp  172.16.1.67:53089          54.240.227.37:80
54.240.227.37:80          192.168.91.24:53384        0      5
NFe0f0r0 NAT      amazon_adsystem
Tcp  172.16.1.67:53229          151.101.90.2:80
151.101.90.2:80           192.168.91.24:53419        300    5
NFe0f0r0 NAT      outbrain
Tcp  172.16.1.67:53076          184.86.235.64:443
184.86.235.64:443         192.168.91.24:3471         300    5
NFe0f0r0 NAT      https
Tcp  172.16.1.67:52971          172.217.160.74:443
172.217.160.74:443        192.168.91.24:3466         300    5
NFe0f0r0 NAT      google_gen
Tcp  172.16.1.67:52829          54.230.214.142:80
54.230.214.142:80         192.168.91.24:53334        300    5
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52934          54.153.178.119:80
54.153.178.119:80         192.168.91.24:53364        300    5
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52794          23.48.137.41:80
23.48.137.41:80           192.168.91.24:53324        300    5
NFe0f0r0 NAT      cnn
Tcp  172.16.1.67:52974          66.235.153.37:80
66.235.153.37:80          192.168.91.24:53374        300    5
NFe0f0r0 NAT      cnn
```

show session gtp

Description display GTP session information.

Syntax `show session gtp`

Mode All

Example The following example shows sample output for the **`show session gtp`** command:

```
ACOS (config)#show session gtp
Traffic Type                                Total
-----------------------------------------------
GTP-C Established                           0
GTP-C Half Open                             0
GTP-U Count                                 0
GTP-C Echo Count                            0
GTP-U Echo Count                            0
GTP Current Available Conn                  203980
GTP Conn Created(cumulative)                0
GTP Conn Freed(cumulative)                  0
```

Field	Description
GTP-C Established	The number GTP-C sessions established.
GTP-C Half Open	The number of GTP-C sessions half-open.
GTP-U Count	The total number of GTP-U sessions.
GTP-C Echo Count	The total number of GTP-C Echo sessions.
GTP-U Echo Count	The total number of GTP-U Echo sessions.
GTP Current Available Conn	The total number of GTP connections currently available. **NOTE:** The number of GTP connections displayed is an approximate value.

Field	Description
GTP Conn Created (cumulative)	The cumulative number of GTP connections created including GTP-C, GTP-U and GTP Echo connections.
GTP Conn Freed (cumulative)	The cumulative number of GTP connections freed.

show system radius server

Description View system RADIUS server information.

Syntax

```
show system radius server {config | statistics}
```

Mode All

Example The following example shows sample output for the **show system radius server config** command:

```
ACOS# show system radius server config
system radius server
remote ip-list client
secret secret-encrypted
37O48xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2w
Dn
attribute inside-ip number 8
attribute inside-ipv6-prefix prefix-length 96 number 97
attribute msisdn number 31
attribute imei vendor 10415 number 20
attribute imsi vendor 10415 number 1
attribute custom1 NAS-IP-Address value hexadecimal number 4
attribute custom2 Connection_PVC vendor 22610 number 43
attribute custom3 xDSL_number vendor 22610 number 44
accounting start replace-entry
accounting stop delete-entry-and-sessions
accounting interim-update replace-entry
```

Example The following example shows sample output for the **show system radius server statistics** command:

```
ACOS# show system radius server statistics
```

```
system RADIUS Server Statistics:
----------------------------------------
MSISDN Received                0
IMEI Received                  0
IMSI Received                  0
Custom Attribute Received      0
RADIUS Request Received        0
RADIUS Request Dropped         0
RADIUS Request Bad Secret Dropped 0
RADIUS Request No Key Attribute Dropped 0
RADIUS Request Malformed Dropped 0
RADIUS Request Ignored         0
RADIUS Request Table Full Dropped 0
RADIUS Secret Not Configured Dropped 0
HA Standby Dropped             0
Framed IPV6 Prefix Length Mismatch 0
Radius Request has Invalid Key Field 0
```

show system radius table

Description View system RADIUS table information.

Syntax

```
show system radius table
[brief | derived-attribute-name {usergroup | userid} derived-
attribute-value value| imei | imsi | inside-ip | inside-ipv6 |
msisdn | attr-name]
```

Parameter	Description
brief	Shows the statistics only.
derived-attribute-name {usergroup | userid} derived-attribute-value *value*	Shows information associated with the RADIUS session based on the specified derived attribute. • **usergroup**: Filters information for the specified value for the user group. • **userid**: Filters information for the specified value for the user

Parameter	Description
	ID. The length of the `derived-attribute-value` can be 1-63.
imei *string*	Shows information associated with the IMEI.
imsi *string*	Shows information associated with the IMSI.
inside-ip	Shows information associated with the inside IP address.
inside-ipv6	Shows information associated with the inside IPv6 address.
msisdn	Shows information associated with the MSISDN.
attr-name	Show information associated with the customized attribute.

Mode All

Example The following command shows sample output for the **show system radius table** command:

```
ACOS# show system radius table
system RADIUS Table Statistics:
-----------------------------------------
Record Created                 3
Record Deleted                 2

Key Attribute        MSISDN       IMEI         IMSI
NAS-IP-Address Connection_PVC xDSL_number     username
                                              domain
                                              Derived-
Attribute User Group
-------------------------------------------------------------------
------------
245.255.255.226     012345678   0123456789  0123456779
ffffe884
```

```
Total RADIUS Records Shown: 1
```

show threat-intel database webroot

Description View details about the threat intelligence database from Webroot.

Syntax

```
show threat-intel database webroot
```

Mode All

Example The following example shows the sample output for **show threat-intel database webroot** command:

```
ACOS(config)# show threat-intel database webroot
Database Name                    : wr_ip_All_1_1479.txt
Database Status                  : Active
Database Size                    : 24 MB
Database Version                 : 1479
Last Update Time                 : Mon Feb 26 11:28:47 2018
Next Update Time                 : Mon Feb 26 15:28:42 2018
Connection Status                : GOOD
Last Successful Connection       : Mon Feb 26 13:28:46 2018

Entries loaded per threat category
spam-sources                     : 444059
windows-exploits                 : 107362
web-attacks                      : 1684
botnets                          : 184306
scanners                         : 136516
dos-attacks                      : 0
reputation                       : 0
phishing                         : 78161
proxy                            : 386170
mobile-threats                   : 2019
tor-proxy                        : 925
all-categories                   : 1266571
```

Field	Description
Database Name	The name of the database file used for

Field	Description
	storing threat intelligence data.
Database Status	This field provides information about whether the database is ready to use. Possible values for this field include: • `Inactive`: No database is loaded in memory. Threat-intel cannot be used in this state. • `Downloading`: A database is currently being downloaded. • `Processing`: Database file is being processed, saving to a file, checksum calculations, etc. • `Loading into memory`: Database is being loaded into memory. • `Active`: Database is loaded and threat-intel module is ready to process traffic.
Database Size	The size of the database file.
Database Version	The version of the database.
Last Update Time	The last time the database file was updated.
Next Update Time	The scheduled time for the next data-base update.
Connection Status	Indicates the status of the connection.
Last Successful Connection	Indicates the time stamp for the last successful connection.

show threat-intel ip-category

Description Show the threat categories associated with the specified IPv4 address.

Syntax `show threat-intel ip-category ipv4-address webroot`

Mode All

NOTE: This command above works only if threat-intel module is enabled and the database status is active.

Example First example output:

```
ACOS(config)# show threat-intel ip-category 8.8.8.8 webroot
Not a threat
```

The response `Not a threat` indicates that the IP address 8.8.8.8 is not associated with any known threats in the Webroot database.

Example Second example output:

```
ACOS(config)# show threat-intel ip-category 1.32.0.0 webroot
spam-sources
mobile-threats
```

The output lists two categories: `spam-sources` and `mobile-threats`, indicating that the IP address 1.32.0.0 is associated with spam activities and threats targeting mobile platforms.

show threat-intel log webroot

Description Show the log for the Webroot threat intelligence module.

Syntax

```
show threat-intel log webroot [ follow | from-start | num-lines num]
```

Paramater	Description
follow	Display the current running threat-intel log for Webroot module.
from-start	Display the threat-intel log from the beginning for the Webroot module.
num-lines *num*	Specify the number of lines to be displayed from the most recent entries in threat-intel log.

Mode All

Example Example output for the **show threat-intel log webroot** command:

```
ACOS(config)# show threat-intel log webroot
2018-02-16 15:40:41 ERROR: Cannot resolve host api.bcti.brightcloud.com:
Temporary failure in name resolution
2018-02-16 15:40:41 ERROR: IpUpdateTask: OnError!
2018-02-16 15:59:40 ERROR: Cannot resolve host api.bcti.brightcloud.com:
Temporary failure in name resolution
2018-02-16 15:59:40 ERROR: IpUpdateTask: OnError!
2018-02-16 17:02:04 ERROR: Cannot resolve host api.bcti.brightcloud.com:
Temporary failure in name resolution
2018-02-16 17:02:04 ERROR: IpUpdateTask: OnError!
```

show threat-intel hits webroot

Description Show the number of hits for each Webroot threat category.

NOTE: On Multi-PU platforms, the counters display aggregated values from PU1 and PU2.

Syntax **show threat-intel hits webroot**

Mode All

Example The following example shows sample output for the **show threat-intel hits webroot** command:

```
ACOS# show threat-intel hits webroot
spam-sources                    : 1
windows-exploits                : 0
web-attacks                     : 0
botnets                         : 0
scanners                        : 0
dos-attacks                     : 0
reputation                      : 0
phishing                        : 0
proxy                           : 0
mobile-threats                  : 1
tor-proxy                       : 0
Total Lookups in Database       : 1
```

```
Total Lookups in RTU cache      : 0
Non malicious IP Lookups        : 15
```

show traffic-control rule-set

Description View Traffic Control rule-set statistics.

Syntax

```
show traffic-control rule-set name
 [ rule-name name ]
```

Parameter	Description
rule-set *name*	View statistics for the Traffic Control rule-set. Specify the rule-set name (1-63 characters).
rule-name *name*	View statistics for the rule from the Traffic Control rule-set. Specify the rule name (1-63 characters).

Mode All

Example The following example shows sample output for **show traffic-control rule-set** command:

```
AX2500(config)# show traffic-control rule-set rate-limit
Rule-Set-Name: rate-limit
Rule-Set-Status: inactive
Total-Rule-Count: 3

Rule-Name:                      1
Status:                         enable
Hit-Count:                      0

Rule-Name:                      2
Status:                         enable
Hit-Count:                      0

Rule-Name:                      3
Status:                         enable
Hit-Count:                      0
```

The following table provides the field descriptions:

Field	Description
Rule-Set-Name	The name of the Traffic Control rule-set
Rule-Set-Status	The status of the rule-set. It can be **active** or **inactive**.
Total-Rule-Count	The total number of rules in the rule-set.
Rule-Name	The name of the rule.
Status	The status of the rule. It can be **enabled** or **disabled**.
Hit-Count	The number of times packets have matched the rule criteria.

clear counters fw rate-limit

Description Clear the counters for Firewall rate limit entries.

Syntax

```
clear counters fw rate-limit
```

Mode All

NOTE: It is recommended not to use this command to clear live rate limit entries.

clear counters threat-intel threat-list

Description Clear the counters for the number of hits for the specified threat-list. This threat-list is configured using the Webroot threat categories.

Syntax

```
clear counters threat-intel threat-list <list-name>
```

Mode All

clear counters threat-intel webroot-global

Description Clear the global counters for the Webroot module.

Syntax

```
clear counters threat-intel webroot-global
```

Mode All

clear fw ddos

Description Clear DDoS protection information.

Syntax

```
clear fw ddos [ statistics | dest ] [ ip-entries | ip-incidents] [ address ipv4-address | all ]
```

Parameter	Description
statistics	Clear DDoS statistics.
dest	Clear DDoS destination entry information.
[ip-entries | ip-incidents] [address *ipv4-address* **| all]**	Clear DDoS destination information for the IP entries or the IP incidents. You can clear the entries or incidents for one of the following: • **address** *ipv4-address* - Clear DDoS destination entry information for the specified IPv4 address. • **all** - Clear DDoS destination entry information for all entries.

Mode All

clear fw ddos-protection

Description Clear firewall DDoS protection entries.

Syntax

```
clear fw ddos-protection entries [ipv4-address | ipv6-address ]
```

Clear the firewall DDoS protection entries for the specified IPv4 or IPv6 address.

Mode All

clear fw full-cone-sessions

Description Clears Firewall full-cone session information for the specified IPv4 or IPv6 address.

Syntax

```
clear fw full-cone-sessions [ipv4-address ipv-addr | ipv6-address ipv6-addr]
```

Mode All

clear fw tcp syn-cookie statistics

Description Clear all statistics for TCP SYN cookies.

Syntax

```
clear fw tcp syn-cookie statistics
```

Mode All

clear fw top-k-rules

Description Clear the statistics related to the most frequently matched firewall rules.

Syntax

```
clear fw top-k-rules metric-name { Permit-Rules | Deny-Rules | Reset-Rules | Stale-Permit-Rules | Stale-Deny-Rules | Stale-Reset-Rules }
```

Parameter	Description
metric-name	Specify the metric for which the firewall rules statistics need to be cleared.
You can specify one of the following options:	
Permit-Rules	Clear the statistics for the top rules that permit the traffic.

Parameter	Description
Deny-Rules	Clear the statistics for the top rules that deny the traffic.
Reset-Rules	Clear the statistics for the top rules that reset the connection or session.
Stale-Permit-Rules	Clear the statistics for the top permit rules that are considered stale, meaning they haven't matched any traffic for a certain period.
Stale-Deny-Rules	Clear the statistics for the top deny rules that are considered stale, meaning they haven't matched any traffic for a certain period.
Stale-Reset-Rules	Clear the statistics for the top reset rules that are considered stale, meaning they haven't matched any traffic for a certain period.

Mode All

Usage Use this command effectively to optimize and refine the firewall rule-set. This command allows you to clear the rules that do not serve the purpose (stale rules).

clear sessions fw helper-sessions

NOTE: This is an internal command. It should only be used by A10 Networks Technical Support for debugging purposes.

Description Clears firewall information for SMP helper sessions.

Syntax

```
clear sessions fw helper-sessions
[ipv4 | ipv6]
```

Parameter	Description
ipv4	This is an optional parameter that allows you to

Parameter	Description
	clear only the IPv4 SMP helper sessions.
ipv6	This is an optional parameter that allows you to clear only the IPv6 SMP helper sessions.

Mode All

Usage If neither the **ipv4** or **ipv6** options are specified, then both IPv4 and IPv6 will be cleared.

Example The following example clears the IPv4 SMP helper sessions:

```
ACOS(config)# clear sessions fw helper-sessions ipv4
```

clear system radius server statistics

Description Clears system RADIUS server statistics.

Syntax

```
clear system radius server statistics
```

Mode All

clear system radius table

Description Clears system RADIUS table information.

Syntax

```
clear system radius table [derived-attribute-name {usergroup | userid} derived-attribute-value value| imei | imsi | inside-ip | inside-ipv6 | msisdn | attr-name]
```

Parameter	Description
derived-attribute-name {user-group | userid} derived-attribute-value [*value*]	Clears information associated with the specified system RADIUS table derived-attribute. The length of the derived-attribute-value can be 1-63.
imei *string*	Clears information associated

Parameter	Description
	with the IMEI.
imsi *string*	Clears information associated with the IMSI.
inside-ip	Clears information associated with the inside IP address.
inside-ipv6	Clears information associated with the inside IPv6 address.
msisdn	Clears information associated with the MSISDN.
attr-name	Clears information associated with the customized attribute.

Mode All

clear tacacs-server statistics

Description Clears the TACACS+ server statistics.

Syntax `clear tacacs-server statistics`

Mode All

NOTE: The clear tacacs-server statistics command resets all TACACS+ server statistics to zero

Example The following example shows sample output for the **clear tacacs-server statistics** command:

```
ACOS(config)# clear tacacs-server statistics
ACOS(config)#
ACOS(config)#
ACOS(config)# show tacacs-server 5.5.5.5
TACACS+ server             :  5.5.5.5:49
               Socket opens:              0
              Socket closes:              0
              Socket aborts:              0
              Socket errors:              0
```

```
            Socket timeouts:                0
    Failed connect attempts:                0
         Total packets recv:                0
         Total packets send:                0
```

clear threat-intel hits webroot

Description Clear the counters for the number of hits for each Webroot threat category.

Syntax

```
clear threat-intel hits webroot
```

Mode All

Next Generation Web Application Firewall

A10 Network's Next Generation Web Application Firewall (NGWAF) is implemented based on A10 ADC capabilities empowered by Fastly (a two-time WAF Gartner visionaries' vendor) technology for identification and mitigation of attacks and bad signals.

NGWAF is an application security monitoring system that monitors suspicious and anomalous web traffic and protects against attacks directed at applications and origin servers. It provides superior protection for applications and APIs by delivering several advantages over legacy WAF.

This reference lists the CLI configuration and show commands that apply specifically to NGWAF.

Configuration Commands

ng-waf

Description Configure A10 Next-Gen WAF (NGWAF) settings.

Syntax

```
[no] ng-waf [ attack-resp-code resp_code | attack-resp-message { msg | custom-page page } | custom-signal-clist string_list | monitor-mode-enable | pre-process-enable exp_time | use-https-proxy { { ipv4_address | ipv6_address } portnum} | use-mgmt-port ]
```

Parameter	Description
attack-resp-code *resp_code*	Specify a custom response code i.e., an HTTP status code (400 to 599) to be returned when a request is blocked by NGWAF.

Parameter	Description
	NOTE: The custom response code on the Fastly Dashboard supersedes this setting i.e., this setting is ignored if you specify a response code on the Fastly Dashboard. By default, a response code 410 is returned if no response code is set on the Fastly dashboard or the Thunder device (using this option).
attack-resp-message *msg* | **custom-page** *page*	Display a custom message when a request is blocked by NGWAF. The message can be displayed by specifying one of the following: • *msg* - A block message with a maximum length of 1023 characters. • **custom-page** *page* - An HTML webpage that contains the message to be displayed. **NOTE:** Ensure that you import the HTML webpage (using **import ng-waf-custom-page** command) to the shared partition or an L3V partition before executing this command. You can also add some relevant information to the message or webpage by using the reserved keywords that display the attack type, the time, the session ID, and the URI as well. The following keywords are available: • **$a10_ngwaf_attack_type$** - The reason for blocking the request or the attack type. For e.g., XSS, SQLI, or custom signals • **$a10_ngwaf_time$** - The time when the request is blocked.

Parameter	Description
	• **$a10_ngwaf_session_id$** - The session ID. • **$a10_ngwaf_uri$** - The request URI. **NOTE:** The keywords are case-sensitive and only 4 keywords can be used in a message or custom webpage.
custom-signal-clist *string_list*	Reserve and track certain custom signals by creating a class-list and binding it to NGWAF. **NOTE:** The class-list cannot have more than 64 entries.
monitor-mode-enable	Enable NGWAF monitor mode. When this mode is enabled, all the requests are monitored and allowed to pass; they are not blocked. However, the malicious requests, that would otherwise be blocked, are highlighted in the Syslogs and debug logs using the **marked** keyword. **NOTE:** The monitor mode overrides the Fastly rules configured to block and redirect requests, i.e., the Fastly rules are ignored when the monitor mode is enabled on the Thunder device.
pre-process-enable *exp_time*	Enable the NGWAF cache function to speed up the processing time. When this option is configured, the checked and forwarded requests are stored in the cache. Thereafter, similar requests are forwarded directly (without NGWAF checking). This option is disabled by default. **NOTE:** Blocked requests are not stored in the cache.

Parameter	Description
	exp_time - Specify the expiration time (1 to 480 minutes) for the cache entries. The default value is 1 minute. Additionally, all cache entries are freed if the partition is disabled or deleted.
use-https-proxy { *ipv4_address* **|** *ipv6_address* **}** *portnum*	Connect to the Fastly Cloud through an explicit proxy server. By default, the connection to the Fastly Cloud is proxy-free. Specify the following parameters: • *ipv4_address* - Proxy server IPv4 address OR *ipv6_address* - Proxy server IPv6 address • *portnum* - The port number (1-65534) **NOTE**: • Ensure that the specified explicit proxy server is reachable. • NGWAF (if enabled) will restart automatically after configuring or deleting the explicit proxy server.
use-mgmt-port	Connect to the Fastly Cloud through the management interface instead of the data interface (default route). **NOTE:** This command is only available on the shared partition but is applied to all partitions.

Default See descriptions.

Mode SLB common configuration mode.

Usage Although this command is under SLB Common, all the sub-commands can also be configured separately for each partition. Therefore, the shared partition and the L3V partitions can have different NGWAF settings.

Example The following example enables the NGWAF cache function and sets the cache expiration time to 5 minutes:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf pre-process-enable 5
```

Example The following example sets the custom attack response code to 456:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-code 456
```

Example The following example enables the NGWAF monitor mode:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf monitor-mode-enable
```

Example The following example sets a custom message to be displayed when a request is denied:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message "The request
is denied!\n"
```

Example The following example sets a custom message using the reserved keyword:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message "The request
is blocked!\n Additional Information\n URI:$a10_ngwaf_uri$,
time:$a10_ngwaf_time$, attack:$a10_ngwaf_attack_type$, session
ID:$a10_ngwaf_session_id$\n"
```

Example output with keywords replaced:

```
The request is blocked!
Additional Information
URI:/pruducts?category=Gifts'--, time:2022-09-20-T06:49:43Z,
attack:SITE-FLAGGED-IP,SQLI, session
id:632962885477430a344ea0ee
```

Example The following example configures a custom webpage to be displayed when a request is denied:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message custom-page
mypage
```

Example The following example creates a class-list and binds it to NGWAF to track custom signals:

```
ACOS(config)# class-list signal_list string
ACOS(config-class list)# str site.login
ACOS(config-class list)# str site.error
ACOS(config-class list)# str site.logout

ACOS(config)# slb common
ACOS(config-common)# ng-waf custom-signal-clist signal_list
```

Example The following example enables connection through the specified IPv4 proxy server:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-https-proxy 192.168.2.2 3128
```

Example The following example enables connection through the specified IPv6 proxy server:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-https-proxy 2022:192::33 3128
```

Example The following example enables management interface usage for NGWAF:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-mgmt-port
```

license-manager ng-waf-module

Description Configure the A10 Next-Gen WAF (NG-WAF) agent by specifying the license keys. You need to register and get the license keys from the Signal Science website.

Syntax

```
license-manager ng-waf-module access-key-id access_key
secret-access-key secret_key
```

NOTE: This is a per-partition command. The NGWAF agent can be configured for a maximum of 8 partitions.

Parameter	Description
access_key	Enter the NG-WAF agent access-key ID (1-64 characters).
secret_key	Enter the NG-WAF agent secret access key ID (1-64 characters).

Mode Configuration mode

NOTE: This command is not synchronized in aVCS. This implies that if you execute the **license manager ng-waf-module** command on PU1, the command is not executed automatically on PU2; it needs to be executed manually on PU2. However, the behavior is different on Multi-PU platforms. In this case, the **license manager ng-waf-module** command is synchronized to PU2, i.e., when this command is executed on PU1, it is automatically executed on PU2 as well.

Example The following example demonstrates the command usage:

```
ACOS(config)# license-manager ng-waf-module access-key-id
aaaaaaa-bbbb-111222233333-ccddd secret-access-key
aaaaaAAAAA111111222222CCCccttrr
```

Show Commands

clear ng-waf cache

Description Clear NGWAF cache entries.

Syntax

```
clear ng-waf cache [ all | virtual_port_name ]
```

Parameter	Description
all	Clear all NGWAF cache entries in this partition.
virtual_port_name	Clear NGWAF cache entries for the specified virtual port.

Mode Global configuration mode

NOTE: All cache entries are cleared automatically if the partition or the virtual port is disabled or deleted. Additionally, the entries are also cleared if NGWAF is disabled.

Example The following command clears all NGWAF cache entries in the current partition:

```
ACOS# clear ng-waf cache all
```

Example The following command clears the NGWAF cache entries for the specified virtual port:

```
ACOS# clear ng-waf cache vip 80
```

show ng-waf

Description Display Next Generation WAF (NGWAF) statistics for the specified parameters.

Syntax

```
show ng-waf [ custom-page | custom-signals | status | virtual_server_name portnum ]
```

Parameter	Description
custom-page	See show ng-waf custom-page.
custom-signal	See show ng-waf custom-signals.
status	See show ng-waf status.
virtual_server_name portnum	See show ng-waf <virtual server> <port>

Default N/A

Mode All

show ng-waf custom-page

Description Display the number of custom webpages. These pages contain the message to be displayed when a request is blocked by NGWAF.

Syntax

```
show ng-waf custom-page
```

Default N/A

Mode All

Example The following example displays custom NGWAF pages:

```
ACOS(config)# show ng-waf custom-page
FILE NAME                                   FILE SIZE (byte)
-----------------------------------------------------------
mypage                                          536
mypage2                                         800
```

clear ng-waf custom-signals

Description Clear all NGWAF custom signals that are being tracked.

Syntax

```
clear ng-waf custom-signals
```

Mode Global configuration mode

NOTE: All signals are cleared except the ones reserved using the class-list.

Example The following command clears NGWAF custom signals:

```
ACOS# clear ng-waf custom-signals
```

show ng-waf custom-signals

Description Display the custom A10 Next-Gen WAF (NGWAF) signals that are currently being tracked. The signals include the signals reserved in

class-list as well as the signals triggered by the blocked requests.

NOTE: On Multi-PU platforms, this command displays custom signals after merging the signals from both PU1 and PU2 and discarding the duplicate entries.

Syntax `show ng-waf custom-signals`

Default N/A

Mode All

Example The following command displays NGWAF custom signals:

```
ACOS(config)# show ng-waf custom-signals
Custom Signals
site.temp-test-001
site.temp-test-002
site.temp-test-003
```

show ng-waf status

Description Display the current status of A10 Next-Gen WAF (NGWAF) on ACOS.

Syntax `show ng-waf status`

Default N/A

Mode All

Usage The information displayed depends upon where the command is executed. If it is executed on the shared partition, the status of NGWAF on all partitions is displayed. However, if it is executed on the L3V partition, only the status of NGWAF on that partition is displayed.

Example In the following example, the command is executed on the shared partition.

```
ACOS(config)# show ng-waf status
Agent Version: 4.22.0

NGWAF Status:            <partition shared>
```

```
Current status:          RUNNING
Agent name:              AX1030-shared
Access key ID:           e9779xxxxxxxxx
Secret access key:       9VF9Uxxxxxxxxx
Control CPU used:        `1 core
Cache entries:           1
Tracked custom signals:  0

NGWAF Status:            <partition p2>
Current status:          DOWN
Agent name:              AX1030-p2
Access key ID:           11111xxxxxxxxx
Secret access key:       2xxxxxxxxxx
Control CPU used:        1 core
Cache entries:           1
Tracked custom signals:  0

NGWAF Status:            <partition p3>
Current status:          DOWN
Agent name:              AX1030-p3
Access key ID:           N/A
Secret access key:       N/A
Control CPU used:        N/A
Cache entries:           0
Tracked custom signals:  0
```

Example In the following example, the command is executed on an L3V partition.

```
ACOS(config)# active-partition p2
ACOS[p2](config)# show ng-waf status
Agent Version: 4.22.0

NGWAF status:            <partition p2>
Current status:          DOWN
Agent name:              AX1030-p2
Access key ID:           11111xxxxxxxxx
Secret access key:       2xxxxxxxxxx
Cache entries:           1
Tracked custom signals:  0
```

Usage On Multi-PU platforms, the statistics display aggregated counters from both PU1 and PU2. The **Cache entries** field shows the sum of the cache entries for both PU1 and PU2. However, the **Tracked custom signals** field shows the sum of the custom signals after discarding the duplicate ones.

Example In the following example, the command is executed on a Multi-PU platform:

```
TH(config)# show ng-waf status
Agent Version: 4.35.0

NGWAF Status:              <partition shared>
Current status:            RUNNING
Agent name:                TH-shared
Access key ID:             e9779xxxxxxxxx
Secret access key:         9VF9Uxxxxxxxxx
Cache entries: 3000
Tracked custom signals: 15
```

Table 15 describes all the possible fields in the command output.

Table 15 : show ng-waf status fields

Field	Description
Agent Version	The version of the NGWAF agent installed. If the agent is not installed, this field displays **N/A**.
Current status	The field indicates the status of NGWAF on the partition. It can have one of the following values: • RUNNING - NGWAF is enabled • DOWN - NGWAF is disabled
Agent name	The NGWAF agent name that can also be seen on the Fastly dashboard.
Access key ID	The masked access key ID of the agent. If the key ID is not provided, this field displays **N/A**.
Secret access key	The masked secret access key of the agent.

Table 15 : show ng-waf status fields

Field	Description
	If the key is not provided, this field displays **N/A**.
Control CPU used	The number of control CPUs allocated for NGWAF within the partition.
Cache entries	The number of entries in the NGWAF cache.
Tracked custom signals	The number of NGWAF signals that are currently being tracked. The signals include the signals reserved in the class-list as well as the signals for client requests. Only the first 64 signals are tracked.

show ng-waf <virtual server> <port>

Description Display A10 Next-Gen WAF (NGWAF) status for the specified virtual server.

NOTE: On Multi-PU platforms, the statistics display aggregated counters from both PU1 and PU2.

Syntax

```
show ng-waf <virtual_server_name> <portnum>
```

Parameter	Description
virtual_server_name	Specify the name of the virtual server (1-128 characters).
portnum	Specify the virtual server port number (1-65534).

Default N/A

Mode All

Example The following example displays the NGWAF statistics for the specified virtual server:

```
ACOS# show ng-waf vip 80
```

```
Requests
 Received                  40
 Redirected                2
 Forwarded                 22
 Blocked                   15
 Error                     3
Attacks
 Command Execution         8
 Cross Site Scripting      3
 Directory Traversal       8
 SQL Injection             3
Anomalies
 Private Files             1
Custom Signals
 site.tp                   2
```

Usage On Multi-PU platforms, the statistics display aggregated counters from both PU1 and PU2 when the command is executed on PU1. However, if the command is executed on PU2, the counters display values from PU2 only.

Example In the following example, the show command is executed on PU1:

```
NGWAF# show ng-waf vs-test-ngwaf 80
Requests
 Received                                7
 Blocked                                 7
Attacks
 SQL Injection                           7
Anomalies
 Blocked Requests                        7

NGWAF# show ng-waf vs-test-ngwaf 443
Requests
 Received                                7
 Blocked                                 7
Attacks
 SQL Injection                           7
Anomalies
 Blocked Requests                        7
```

In the following example, the show command is executed on PU2:

```
NGWAF-UNIT-1# show ng-waf vs-test-ngwaf 80
Requests
 Received                                3
 Blocked                                 3
Attacks
 SQL Injection                           3
Anomalies
 Blocked Requests                        3

NGWAF-UNIT-1# show ng-waf vs-test-ngwaf 443
Requests
 Received                                3
 Blocked                                 3
Attacks
 SQL Injection                           3
Anomalies
 Blocked Requests                        3
```

describes all the possible fields in the command output.

Table 16 : show ng-waf fields

Field	Description
Requests	Counters for the HTTP requests processed: • Received - The total number of HTTP requests received. It is the sum of the Forwarded, Blocked, Bypassed, and Erroneous requests. • Redirected - The number of HTTP requests blocked and redirected. • Forwarded - The number of HTTP requests forwarded. • Blocked - The number of HTTP requests blocked. • Bypassed - The number of HTTP requests bypassed. The requests are bypassed when the request matches the NGWAF cache or when the NGWAF service is restarted.

Table 16 : show ng-waf fields

Field	Description
	• Error - The number of errors occurred while processing the requests. • Marked - The number of HTTP requests highlighted as **`marked`** when NGWAF monitor mode is enabled.
Attacks	Counters for the attacks: • Attack Tooling - The number of Attack Tooling attacks detected. • AWS SSRF - The number of Server Side Request Forgery (SSRF) attacks detected to obtain Amazon Web Services (AWS) keys and gain access. • Backdoor - The number of Backdoor Signal attacks detected. • Command Execution - The number of Command Execution attacks detected. • Cross Site Scripting - The number of Cross Site Scripting attacks detected. • Directory Traversal - The number of Directory Traversal attacks detected. • GraphQL Max Depth - The number of requests that reach or exceed the maximum depth allowed on the server for GraphQL API queries. • Log4J JNDI - The number or Log4J JNDI attacks that attempt to exploit the Log4Shell vulnerability (present in Log4J versions earlier than 2.16.0). • SQL Injection - The number of SQL Injection attacks detected.
Anomalies	Counter for the anomalous requests: • Abnormal Path - The number of times the original path differs from the normalized path.

Table 16 : show ng-waf fields

Field	Description
	• Bad Hop Headers - The number of HTTP smuggling attempts. • Blocked Requests - The number of requests blocked by Signal Science. • Code Injection PHP - The number of requests where PHP code commands are used to gain control or damage a target system. • Compression Detected - The number of requests where the POST request body is compressed and cannot be inspected. • Datacenter Traffic - The number of non-organic requests that originate from identified host providers. • Double Encoding - The number of double-encoded requests. • Duplicate Header Names - The number of requests having duplicate header field names. • Forceful Browsing - The number of failed attempts to access admin pages. • GraphQL Duplicate Variables - The number of requests that contain duplicated variables. • GraphQL IDE - The number of requests originating from a GraphQL Interactive Development Environment (IDE). • GraphQL Introspection - The number of attempts to obtain the schema of a GraphQL API. The schema can be used to identify which resources are available, thereby informing subsequent attacks. • GraphQL Max Depth - The number of requests that reached or exceeded the maximum depth allowed

Table 16 : show ng-waf fields

Field	Description
	on the server for GraphQL API queries. • GraphQL Missing Required Operation Name - The number of requests that have multiple GraphQL operations but do not define which operation to execute. • GraphQL Undefined Variable - The number of requests made to a GraphQL API containing undefined variables that are not expected by the function. • HTTP 403 Errors - The number of requests resulting in an HTTP 403 (Forbidden error) status code. • HTTP 404 Errors - The number of requests resulting in an HTTP 404 (Not Found error) status code. • HTTP 429 Errors - The number of requests resulting in an HTTP 429 (Too Many Requests) status code. • HTTP 4XX Errors - The number of requests resulting in HTTP 4xx errors (other than 403, 404, and 429) commonly known as client request errors. • HTTP 500 Errors - The number of requests resulting in an HTTP 500 (Internal Server Error) status code. • HTTP 503 Errors - The number of requests resulting in an HTTP 503 (Service Unavailable) status code. • HTTP 5XX Errors - The number of requests resulting in HTTP 5xx errors (other than 500 and 503) commonly known as server related issues. • HTTP Response Splitting - The number of requests where CRLF characters are submitted as input to the application to inject headers into the HTTP response. • Invalid Encoding - The number of requests with

Table 16 : show ng-waf fields

Field	Description
	Invalid Encoding. • JSON Encoding Error - The number of requests with JSON encoding error. • Malformed Data in the response body - The number of requests with a malformed POST, PUT, or PATCH request body. • Malicious IP Traffic - The number of requests from IP addresses with malicious activity. • Missing Content-Type request header - The number of POST, PUT, or PATCH request types that do not have Content-Type request header. • Network Effect - The number of subsequent requests from IPs that were marked malicious previously. • No User Agent - The number of automated and malicious requests using fake or missing User-Agents. • Null Byte - The number of requests with Null Bytes (malformed requests). • Private Files - The number of requests with private files that could leak sensitive information. • Scanner - The number of requests that identify popular scanning services and tools. • SearchBot Impostor - The number of requests with Search bot impostors. • Site Flagged IP - The number of requests received from an IP that was flagged for exceeding attack thresholds for a specific site. • Tor Traffic - The number of requests with Tor traffic that conceals user's identity.

Table 16 : show ng-waf fields

Field	Description
	• Weak TLS - The number of requests with weak TLS connections. • XML Encoding Error - The number of requests with XML encoding errors. • Other - The number of requests other than those mentioned above.
Custom Signals	Counters for the custom signals that are triggered when requests are blocked. Only the first 64 signal counters are displayed; the later counters (65th and above) are counted as **Unknown**.

For more details, refer to https://docs.fastly.com/signalsciences/faq/system-tags/.

Security Gateway

ACOS software supports Internet Protocol Security (IPsec) Virtual Private Network (VPN). IPsec VPN is a suite of protocols that secures private traffic over a public network. To protect communications, organizations need to encrypt data at high speeds and scale-out VPN tunnel capacity on-demand. ACOS uses IPsec VPN to secure high-capacity links at unparalleled speeds.

This reference lists the CLI configuration and show commands that apply specifically to IPsec.

Configuration Commands

pki acme-cert

Description Creates a certificate enrolment name using the Automatic Certificate Management Environment (ACME) protocol.

Syntax

```
pki acme-cert name {account-email | cert-type | domain | other options}
```

Parameter	Description
name	Specify the name of the certificate. `ACOS (config)# pki acme-cert test`
account-email	Specify a valid email address for the ACME account. The CA certificate uses this email address to send the expiration notices and issues reported. `ACOS (config-acme cert:test)# account-email exampleuser@exampledomain.com`
acme-client	Specify the ACME client for the ACME enrollment or renewal. The following options

Parameter	Description
	can be configured: • `agent-v1` - Sets `agent-v1` as the ACME client. The default is agent-v1. • `agent-v2` - Sets `agent-v2` as the ACME client. `ACOS (config-acme cert:test)# acme-clientagent-v1`

cert-type *{rsa | ecdsa}*	Specify the certificate type.
	The following options can be configured:
	• `rsa` - Enable RSA certificate along with the rsa-key-length private key size for the device certificate in bits. By default, the value is set to 2084.
	`ACOS (config- acme cert:test)# cert-type rsa rsa-key-length 2084`
	• `ecdsa` - Enable ECDSA certificate along with the ec-key-length private key size for the device certificate in bits. By default, the value is set to 384.
	`ACOS (config- acme cert:test)# cert-type ecdsa ec-key-length384`

device-context	Specify the device context to switch to a particular device for VCS config.
domain	Specify the domain name for which you want to issue the CA certificate. The CA server will verify whether you control this domain. `ACOS (config- acme cert:test)# domain exampledomain.com`
eab-hmac-key *{name* | **encryp-**	Specify the HMAC key for ACME External Account Binding (EAB).

Parameter	Description
ted *name}*	The MAC key should be in base64url-encoded format. • *name* - Specify the HMAC key. • **encrypted** *name* - Specify the A10 reserved encrypted password. Do not use this option manually. `ACOS (config- acme cert:test)# eab-hmac-key _bn_xA1sxtf7Nd1-lJWHLa24GCy8mwDEfYvehJmxRVWFdJ-41BOQNdN9Q-JtTQYKZyUDjNfU7Aen_6DJ22gYA`
eab-key-id *name*	Specify the key identifier for ACME EAB. The key identifier must be an ASCII string. `ACOS (config- acme cert:test)# eab-key-id OBUBsbgSqLa5_Iw9EnbC7g`
enroll	Initiate the device enrollment (staging or force) with the CA certificate. `ACOS (config- acme cert:test)# enroll`
run-with-staging-server	Run the ACME operation with the staging server. **NOTE:** Due to the CA rate limitation, A10 strongly recommends you run this option first while you test the configuration.
force	Able to do the enrollment again. In the ACME certificate, the **force** option will be automatically enabled for the renewal.
log-level *{1 | 2}*	Specify the logging level output of the ACME commands.

Parameter	Description
	The following options can be configured: • `1` - Enable the default and basic logging level. • `2` - Enable the detailed logging level, which includes debugging messages. `ACOS (config- acme cert:test)# log-level 2`
verification-waiting-time	Specify how long (in seconds) the ACME client should wait for the CA certificate to verify the challenge token.
renew-before *{hour | day | week | month}*	Specify the periodic interval to renew automatically before the certificate expires. The following periodic interval options are available: • `hour` • `day` • `week` • `month` (one month = 30 days) `ACOS (config- acme cert:test)# renew-before month 1`
renew-every *{minute | hour | day | week | month}*	Specify the periodic interval in which the certificate must be renewed. The following periodic interval are available: • `minute` • `hour` • `day` • `week` • `month (one month = 30 days)`

Parameter	Description
	`ACOS (config- acme cert:test)# renew-every hour 8`
san-domain *{dns}*	Specify the Subject Alternate Name (SAN) to use it while enrolling the certificate and specify the hostname of the subject. `ACOS (config- acme cert:test)# san-domain test.com`
url	Specify the ACME directory URL. By default, use Let's encrypt as a CA server. The format is: http (s)://host:[port]/path `ACOS (config- acme cert:test)# url https://www.caserver.com/testing`
staging-url	Specify the ACME staging directory URL. By default, use Let's encrypt as a CA server. The format is: http(s)://host:[port]/path. `ACOS (config- acme cert:test)# staging-url https://www.caserver.com/staging`
vrid	Specify the high availability VRRP-A VRID, which will be used to sync the HTTP-01 challenge token. **NOTE:** You must configure aVCS and VRRP-A, if you want to use ACME to get the domain cert with the same CN on multiple boxes. `ACOS (config- acme cert:test)# vrid 1`

Mode Configuration mode

Example The following command shows the example to set ACME certificate:

```
ACOS(config)# pki acme-cert test
```

```
ACOS(config-acme cert:test)# eab-hmac-key _bn_xA1sxtf7Nd1-
lJWHLa24GCy8mwDEfYvehJmxRVWFdJ-41BOQNdN9Q-JtTQYKZyUDjNfU7Aen_
6DJ22gYA
ACOS(config-acme cert:test)# eab-key-id OBUBsbgSqLa5_Iw9EnbC7g
ACOS(config-acme cert:test)# account-email test@url.com
ACOS(config-acme cert:test)# acme-client agent-v1
ACOS(config-acme cert:test)# cert-type rsa
ACOS(config-acme cert:test)# domain test.com
ACOS(config-acme cert:test)# san-domain testing.com
ACOS(config-acme cert:test)# url
https://www.caserver.com/testing
ACOS(config-acme cert:test)# enroll
ACOS(config-acme cert:test)# run-with-staging-server
ACOS(config-acme cert:test)# renew-every hour 8
ACOS(config-acme cert:test)# exit
```

account-email

Description Specify a valid email address for the ACME account. The CA certificate uses this email address to send the expiration notices and issues reported. You can specify 1-64 characters.

Syntax

```
[no] account-email
```

Default N/A

Mode ACME certificate mode

acme-client

Description Specify the ACME client for the ACME enrolment or renewal. The default option is `agent-v1`.

Syntax

```
[no] acme-client {agent-v1 | agent-v2}
```

Parameter	Description
agent-v1	Sets agent-v1 as the ACME client for the ACME enrolment or renewal. This is the default value.
agent-v1	Sets agent-v2 as the ACME client for the ACME enrolment or renewal.

Default agent-v1

Mode ACME certificate mode

enroll

Description Initiates enrollment of device with the CA. Due to CA rate limit, A10 recommends to set "run-with-staging-server" during test.

Syntax

```
[no] enroll
```

Default Disabled

Mode ACME certificate mode

log-level

Description Specify the level for logging output of ACME commands (default 1 and detailed 2).

Syntax

```
[no] log-level level
```

Parameter	Description
level	Level for logging output of ACME commands. It is <1-2> level.

Default 1

Mode ACME certificate mode

renew-before

Description Specify interval before certificate expiry to renew the certificate.

Syntax

```
[no] renew-before {hour | day | week | month}
```

Parameter	Description
hour	Number of hours before the certificate expiry. The value of renewal period is between 1-255.
day	Number of days before the certificate expiry. The

Parameter	Description
	value of renewal period is between 1-255.
week	Number of weeks before the certificate expiry. The value of renewal period is between 1-255.
month	Number of months before the certificate expiry (1 month = 30 days). The value of renewal period is between 1-255.

Default N/A

Mode ACME certificate mode

renew-every

Description Specify periodic intervals before certificate expiry to renew the certificate.

Syntax

```
[no] renew-every {minute | hour | day | week | month}
```

Parameter	Description
minute	Periodic interval in minutes. It is between 2-255.
hour	Periodic interval in hours. It is between 1-255.
day	Periodic interval in days. It is between 1-255.
week	Periodic interval in weeks. It is between 1-255.
month	Periodic interval in months. It is between 1-255.

Default N/A

Mode ACME certificate mode

run-with-staging-server

Description Runs ACME operation with the staging server. Due to the CA rate limitation, A10 strongly recommends you to run this option first while you test the configuration.

Syntax

```
[no] run-with-staging-server
```

Default N/A

Mode ACME certificate mode

url

Description Specify the ACME directory URL. By default, use Let's encrypt as a CA server. The format is: http(s)://host:[port]/path.

Syntax

```
[no] url
```

Default N/A

Mode ACME certificate mode

pki acme-concurrent-process-count

Description Configures the number of concurrent ACME processes. The default and the maximum number are dependent on the number of control CPU.

Syntax

```
[no] pki acme-concurrent-process-count <num>
```

Parameter	Description
num	The concurrent ACME processes number. The value can be 1 to 51.

Mode Global configuration

Usage The default and the maximum numbers of ACME concurrent processes depend on the number of control CPUs. If the number of control CPUs is greater than 12, the default and the maximum numbers of ACME concurrent processes are limited to the numbers of 12 control CPUs.

The formula: Default: (<# of ctrl CPU> * 5) - (<# of ctrl CPU> - 1)

Max: <# of default> + 2

No. of control CPUs	Default # of concurrent process	Maximum # of concurrent process
1	5	7

No. of control CPUs	Default # of con-current process	Maximum # of con-current process
2	9	11
3	13	15
4	17	19
5	21	23
6	25	27
7	29	31
8	33	35
9	37	39
10	41	43
11	45	47
12	49	51
# > 12	49	51

Example The following command sets number of concurrent processes to 5:

```
ACOS(config)# pki acme-concurrent-process-count 5
```

Example The following command displays the error message if an invalid ACME concurrent process number is set:

```
ACOS(config)# pki acme-concurrent-process-count 8
Invalid ACME concurrent process number. The default number is
5, and the maximum number is 7 according to the number of
control CPU
```

pki copy-cert

Description Make a copy of the SSL certificate file.

Syntax

```
pki copy-cert source-cert-name [rotationnum] dest-cert-name
[overwrite]
```

Parameter	Description
source-cert-name	Name of the existing SSL certificate file (1-63 characters).
rotation	Specify the rotation number of the SCEP generated certificate file (1-4).
dest-cert-name	Name of the copy of the SSL certificate file (1-63 characters).
overwrite	if there is an existing file with the same name as the specified *dest-cert-name*, overwrite the existing file.

Mode Configuration mode

Example Create a copy of the existing SSL cert file (example_existing_cert.crt) to a new file (example_new_cert.crt), and overwrite the destination file if it has the same name:

```
ACOS(config)# pki copy-cert example_existing_cert.crt example_
new_cert.crt overwrite
```

pki copy-key

Description Makes a copy of the SSL key file.

Syntax

```
pki copy-key source-key-name [rotationnum] dest-key-name
[overwrite]
```

Parameter	Description
source-cert-name	Name of the existing SSL key file (1-63 characters).
rotation	Specify the rotation number of the SCEP generated key file (1-4).
dest-cert-name	Name of the copy of the SSL key file (1-63 characters).
overwrite	if there is an existing file with the same name as the specified *dest-key-name*, overwrite the existing file.

Mode Configuration mode

Example Create a copy of the existing SSL key file (example_existing_key.key) to a new file (example_new_key.key), and overwrite the destination file if it has the same name:

```
ACOS(config)# pki copy-key example_existing_key.key example_
new_key.key overwrite
```

pki cmp-cert

Description Creates a CMP certificate enrollment object.

Syntax

```
pki cmp-cert object-name
```

Replace *object-name* with the name of the certificate you want to enroll (1-63 characters).

Mode Configuration mode

cert-type

Description Specify the certificate type.

Syntax

```
[no] cert-type
```

Parameter	Description
rsa	Enables RSA certificate along with the rsa-key-length private key size for the device certificate in bits. By default, the value is set to 2048.
ecdsa	Enables ECDSA certificate along with the ec-key-length private key size for the device certificate in bits. By default, the value is set to 384.

Default RSA Certificate

Mode CMP certificate mode

cmp-ca

Description The specific CA to trust while verifying signature of CMP response message.

Syntax

```
[no] cmp-ca name
```

Parameter	Description
name	The name of the CA for verifying signature of CMP response message. It can be 1-245 characters.

Default N/A

Mode CMP certificate mode

cmp-cert

Description Specify the CMP server certificate to use and directly trust when verifying the signature of the CMP response message.

Syntax

```
[no] cmp-cert name
```

Parameter	Description
name	The specific name of the CMP server certificate to use and directly trust when verifying the signature of the CMP response message. It can be 1-245 characters.

Default N/A

Mode CMP certificate mode

log-level

Description Specify the level for logging output of CMP commands (default 1 and detailed 2).

Syntax

```
[no] log-level level
```

Parameter	Description
level	Level for logging output of ACME commands. It is 1-2 level.

Default 1

Mode CMP certificate mode

max-polltime

Description Maximum time in seconds an enrollment or a key update may take.

Syntax

```
[no] max-polltime seconds
```

Parameter	Description
seconds	The maximum time in seconds. It can be 5-1024. The default is 120 seconds.

Default 120 seconds

Mode CMP certificate mode

recipient-dn

Description Specify the distinguished name of the CMP message recipient, which is the CMP server. It can be a CA or RA entity.

Syntax

```
[no] recipient-dn {OID}
```

Parameter	Description
OID	The distinguished name OID is case-sensitive. It can be between 2-127 characters.

Default N/A

Mode CMP certificate mode

renew-before

Description Specify interval before certificate expiry to renew the certificate.

Syntax `[no] renew-before {hour | day | week | month}`

Parameter	Description
hour	Number of hours before the certificate expiry. The value of renewal period is between 1-255.
day	Number of days before the certificate expiry. The value of renewal period is between 1-255.
week	Number of weeks before the certificate expiry. The value of renewal period is between 1-255.
month	Number of months before the certificate expiry (1 month = 30 days). The value of renewal period is between 1-255.

Default N/A

Mode CMP certificate mode

renew-every

Description Specify periodic intervals before certificate expiry to renew the certificate.

Syntax `[no] renew-every {minute | hour | day | week | month}`

Parameter	Description
minute	Periodic interval in minutes. It is between 2-255.
hour	Periodic interval in hours. It is between 1-255.
day	Periodic interval in days. It is between 1-255.
week	Periodic interval in weeks. It is between 1-255.
month	Periodic interval in months. It is between 1-255.

Default N/A

Mode CMP certificate mode

secret

Description Specify the pre-shared secret used to enroll the device's certificate.

Syntax `[no] secret name`

Parameter	Description
name	The pre-shared secret. It can be 1-127 characters.

Default N/A

Mode CMP certificate mode

subject-alternate-name

Description Specify the Subject Alternate Name to use while enrolling the certificate

Syntax `[no] subject-alternate-name {dns | email | ip}`

Parameter	Description
dns	Enter the hostname of the subject. It can be 1-127 characters.
email	Enter the email address of the subject. It can be 1-127 characters.
ip	Enter the IP address of the subject. It can be 1-127 characters.

Default N/A

Mode CMP certificate mode

pki create

Description Create security certificate or Certificate Signing Request (CSR).

Syntax
```
pki create certificate mycert certtype
pki create csr csr-name
```

Parameter	Description
certtype	Specify the encryption algorithm to be used.

Parameter	Description
	• rsa - RSA certificate • ecdsa - ECDSA certificate
`csr csr-name`	Specify the Certificate Signing Request (CSR). The csr-name can be user-defined 1-254 characters.

Mode Global configuration

Description PKI SCEP certificate enrollment object.

Syntax

```
pki scep-cert
```

Mode Global configuration

pki delete

Description Deletes a self-signed certificate.

Syntax

```
pki delete {
certificate {cert-name | ca cert-name} |
crl crl-file-name | csr csr-file-name
private-key priv-key-name |
}
```

Commands	Descriptions
certificate	Deletes a specific self-signed certificate name or CA certiticate.
crl	Deletes a specific certificate revocation list (CRL) file.
csr	Deletes a specific Certificate Signing Request (CSR) file.
private-key	Deletes a specific private key.

Mode Configuration Mode

Example The following example deletes the CA certificate.

```
ACOS(config)#pki delete certificate ca CACert
```

NOTE:

The 'a10_autoupdate_ca' CA file can be removed using **pki delete certificate ca a10_autoupdate_ca** only if:

- Other configuration objects are not using it
- **automatic-update ca-bundle schedule** is not configured

pki renew-self

Description Renews a self-signed certificate.

Syntax **pki renew-self** *cert-name* {**days** *num* | **days-others**}

Commands	Description
cert-name	Deletes a specific self-signed certificate.
days *num*	Number of effective dates for which the certificate should be extended. This should be a value from 30 to 3650 days. The default value is a 730 day extension
days-others	Presents a more extensive set of input options. After entering the value for an option, press Enter to display the input prompt for the next option. The following specifications will be presented sequentially: input valid days, 30-3650, default 730: num • input Common Name, 0-64: name • input Division, 0-31: division-name • input Organization, 0-63: organization-name • input Locality, 0-31: city-or-region • input State or Province, 0-31: state-or-province • input Country, 2 characters: country-code

Commands	Description
	• input email address, 0-64: email-address The num specifies the number of effective days for which the certificate should be extended, ranging from 30 to 3650 days. If this field is left blank, then the default value is a 730 day extension. Every other option can be left blank, except for the country-code value. The numbers following Common Name, Division, Organization, Locality, State or Province, and email address specify the number of characters allowed.

Mode Configuration Mode

pki scep-cert

Description Create an SCEP certificate enrollment object.

Syntax

```
pki scep-cert object-name
```

Replace *object-name* with the name of the certificate you want to enroll (1-63 characters).

Mode Configuration mode

dn

Description Specify the Distinguished-Name to use while enrolling the certificate (Format: "cn=user, dc=example, dc=com").

Syntax

```
[no] dn name
```

Parameter	Description
name	Specify the name of the certificate. It can be 1 - 127 characters.

Default Disabled

Mode SCEP certificate mode

enroll

Description Initiates enrollment of device with the CA.

Syntax

```
[no] enroll
```

Default Disabled

Mode SCEP certificate mode

interval

Description Interval time in seconds to poll when SCEP response is PENDING.

Syntax

```
[no] interval seconds
```

Parameter	Description
seconds	Interval time in seconds to poll when SCEP response is PENDING, 1-3600.

Default 5 seconds

Mode SCEP certificate mode

key-length

Description Key length in bits.

Syntax

```
[no] key-length bit key
```

Parameter	Description
bit key	1024, 2048, or 4096 bits.

Default N/A

Mode SCEP certificate mode

log-level

Description Specify the level for logging output of SCEP client commands (default 1 and detailed 4).

Syntax `[no] log-level level`

Parameter	Description
level	<1-4>.

Default N/A

Mode SCEP certificate mode

max-polltime

Description Maximum time in seconds to poll when SCEP response is PENDING.

Syntax `[no] max-polltime seconds`

Parameter	Description
seconds	<15-432000>.

Default 180 seconds

Mode SCEP certificate mode

method

Description HTTP request method used for enrollment.

Syntax `[no] method {GET | POST}`

Parameter	Description
seconds	<15-432000>.

Default N/A

Mode SCEP certificate mode

password

Description Specify the password used to enroll the device's certificate.

Syntax

```
[no] password password
```

Parameter	Description
password	Specify the password used to enroll the device's certificate.

Default N/A

Mode SCEP certificate mode

renew-before

Description Specify interval before certificate expiry to renew the certificate.

Syntax

```
[no] renew-before {day | hour | month | week}
```

Parameter	Description
day	Units of time, 1-255.
hour	Units of time, 1-255.
month	Units of time, 1-255.
week	Units of time, 1-255.

Default N/A

Mode SCEP certificate mode

renew-every

Description Specify interval before certificate expiry to renew the certificate

Syntax

```
[no] renew-every {minute | hour | day | week | month}
```

Parameter	Description
minute	Periodic interval in minutes, 2-255.

Parameter	Description
hour	Periodic interval in hours, 1-255.
day	Periodic interval in days, 1-255.
week	Periodic interval in weeks, 1-255.
month	Periodic interval in months, 1-255.

Default N/A

Mode SCEP certificate mode

subject-alternate-name

Description Specify the Subject Alternate Name to use while enrolling the certificate

Syntax

```
[no] subject-alternate-name {dns | email | ip}
```

Parameter	Description
dns	Units of time, 1-255.
email	Units of time, 1-255.
ip	Units of time, 1-255.

Default N/A

Mode SCEP certificate mode

san-domain

Description Specify the Subject Alternate Name (SAN) to use it while enrolling the certificate and specify the hostname of the subject.

Syntax

```
[no] san-domain {dns}
```

Default N/A

Mode ACME certificate mode

system ipsec crypto-core

Description Assign CPUs for the IPsec processing.

Syntax `[no] system ipsec crypto-core num`

Parameter	Description
num	Number of crypto cores assigned for the IPsec processing, 0-64.

Default N/A

Mode Global configuration mode

system ipsec crypto-mem

Description Assign crypto memory percentage for the IPsec processing.

Syntax `[no] system ipsec crypto-mem num`

Parameter	Description
num	Crypto memory percentage assigned for the IPsec processing, 0-100.

Default N/A

Mode Global configuration mode

system ipsec fpga-decrypt

Description Enable or disable FTA decryption offload.

Syntax `[enable/disable] system ipsec fpga-decrypt`

Default N/A

Mode Global configuration mode

system ipsec packet-round-robin

Description Enable packet round robin for the IPsec packets.

Syntax `[no] system ipsec packet-round-robin`

Default N/A

Usage Global configuration mode

vpn asymmetric-flow-support

Description Enable asymmetric flow support for the IPsec tunnels.

Syntax `[no] vpn asymmetric-flow-support`

Default Disabled

Mode Global configuration mode

vpn extended-matching

Description Enables session extended matching for packets coming from the IPsec tunnel.

Syntax `[no] vpn extended-matching`

Default Disabled

Mode Global configuration mode

vpn fragment-after-encap

Description Configure fragmentation of packets after encapsulation in the IPsec tunnel headers.

Syntax `[no] vpn fragment-after-encap`

Default Disabled

Mode Global configuration mode

vpn ike-logging-enable

Description After enabling the command, the VPN IKE negotiation log is sent to the syslog server. The log can then be viewed using the 'show log' command .

Syntax

```
[no] vpn ike-logging-enable
```

Default Disabled

Mode Global configuration mode

vpn ike-gateway

Description Configure an IKE-based VPN gateway. This command changes the CLI to the configuration level for the specified IKE gateway.

Syntax

```
[no] vpn ike-gateway gateway-name
```

Parameter	Description
vpn ike-gateway	IKE-gateway name is <length:1-31>
gateway-name	Name of the VPN gateway, 1-63 characters.

Default N/A

Mode Global configuration mode

auth-method

Description Chooses the authentication method for IKE phase 1. The same authentication method must also be configured on the peer VPN gateway.
Specifies the hash algorithm to be used for signature authentication (only for IKEv2).

Syntax

```
[no] auth-method {preshare-key string | rsa-signature hash |
ecdsa-signature hash | eap-radius | eap-tls}
```

Parameter	Description
preshare-key *string*	Uses the string you enter as the key. The same key value must be configured on the local VPN gateway in ACOS and on the remote gateway.
rsa-signature *hash*	Uses RSA certificate-based authentication to authenticate the remote gateway. • *hash* - Specifies hash algorithm to be used for signature authentication (only for IKEv2). You can specify the following hash algorithms: ◦ sha256 - Secure Hash Algorithm 256 ◦ sha384 - Secure Hash Algorithm 384 ◦ sha512 - Secure Hash Algorithm 512
ecdsa-signature *hash*	Uses an ECDSA certificate-based authentication to authenticate the remote gateway. • *hash* - Specifies hash algorithm to be used for signature authentication (only for IKEv2). You can specify the following hash algorithms: ◦ sha256 - Secure Hash Algorithm 256 ◦ sha384 - Secure Hash Algorithm 384 ◦ sha512 - Secure Hash Algorithm 512
eap-radius	Uses an EAP Radius Server based authentication to authenticate the remote gateway.
eap-tls	Uses an EAP TLS based authentication to authenticate the remote gateway.

Default Preshared key

Mode IKE Gateway mode

Example The following command specifies the hash algorithm (sha256) for signature authentication (only for IKEv2):

```
ACOS(config-ike-gateway:a1)#auth-method ecdsa-signature hash
256
```

configuration-payload

Description The configuration payload is an Internet Key Exchange (IKE) version 2 feature used to proliferate the facilitating data from an IKE responder to the IKE originator. It is supported with route-based VPNs only. It is a single IKE gateway, which accepts the IKE connections from a group of peers. The IKE gateway uses configuration payload to assign the IP address, netmask, gateway, and other parameters.

Syntax

```
[no] configuration-payload {dhcp| radius}
```

Parameter	Description
dhcp	Enables Dynamic Host Configuration Protocol (DHCP) server to retrieve the configuration information.
radius	Enables RADIUS server to retrieve the configuration information.

Default N/A

Mode IKE Gateway mode

Usage This helps to assign the IP address, netmask, gateway, and other parameters.

dh-group

Description The DH group controls the strength of the keying material exchanged during initiation of the IKE SA. During this phase, the devices at each end of the VPN tunnel use the keying materials to generate the public (shared) key, and their own private keys. Higher DH groups provide stronger keying material than lower-numbered groups. Accordingly, higher DH groups also require more processing power than lower-numbered groups.

Syntax

```
[no] dh-group group-num
```

Parameter	Description
group-num	• 1 – Diffie-Hellman group 1– 768-bit (Default) • 2 – Diffie-Hellman group 2 - 1024-bit

Parameter	Description
	• 5 - Diffie-Hellman group 5 - 1536-bit • 14 - Diffie-Hellman group 14 - 2048-bit • 15 - Diffie-Hellman group 15 - 3072-bit • 16 - Diffie-Hellman group 16 - 4096-bit • 18 - Diffie-Hellman group 18 - 8192-bit • 19 - Diffie-Hellman group 19 - 256-bit Elliptic Curve • 20 - Diffie-Hellman group 20 - 384-bit Elliptic Curve.

Default 1

Mode IKE Gateway mode

dpd

Description Configures Dead Peer Detection (DPD). DPD tests idle VPN sessions to ensure the session peer is still responsive.

Syntax

```
[no] dpd interval seconds retry num
```

Parameter	Description
seconds	Specify the number of seconds between DPD R-U-THERE messages. The range can be 1-3600 seconds.
num	Specify the maximum number of times the ACOS resends an unanswered R-U-THERE packet before determining that the tunnel is down. The retries (num) can be 1-10.

Default N/A

Mode IKE Gateway mode

Usage This command helps to detect if the peer VPN gateway is down. Based on the configured DPD interval and the number of retries, the R-U-

THERE message is sent to the remote gateway.
If there is no response from the remote gateway for the configured number of retries, the IKE SAs and any IPsec SAs associated with the peer gateway are deleted.

Example The following example shows the configuration of DPD with interval 10 and retry 3.

```
ACOS-Active(config)#vpn ike-gateway 1
ACOS-Active(config-ike-gateway:1)#dpd interval 10 retry 3
ACOS-Active(config-ike-gateway:1)#exit
```

encryption

Description Algorithm groups specify the encryption settings for IKE. A gateway can have up to four algorithm groups. During SA negotiation, one of the configured algorithm groups is selected.

Syntax

```
[no] encryption encrypt-alg hash hash-alg {priority num}
```

OR

```
[no] encryption encrypt-alg prf prf-alg {priority num}
```

Parameter	Description
encrypt-alg	Specify the encryption algorithm to be used. • **des** - Data Encryption Standard (DES) is a cryptographic algorithm with a 56-bit key. • **3des** - Triple DES is a more powerful version of DES that uses a 168-bit key. • **aes-128** - Advanced Encryption Standard (AES) is more efficient cryptographic algorithm with a 128-bit key. • **aes-192** - AES algorithm that uses a more powerful 192-bit key. • **aes-256** - The most powerful AES algorithm that uses a 256-bit key. • **aes-gcm-128** - Advanced Encryption Standard

Parameter	Description
	algorithm Galois/Counter Mode (key size: 128 bits, ICV size: 16 bytes). • **aes-gcm-192** - Advanced Encryption Standard algorithm Galois/Counter Mode (key size: 192 bits, ICV size: 16 bytes). • **aes-gcm-256** - Advanced Encryption Standard algorithm Galois/Counter Mode (key size: 256 bits, ICV size: 16 bytes). **NOTE:** aes-gcm-128, aes-gcm-192,and aes-gcm-256 are supported in IKEv2 Gateway only. • **null** - No encryption.
hash-alg	Specify the hashing algorithm to be used. • **md5** - Message Digest Algorithm 5 (MD5) is a hashing algorithm that produces a 128-bit hash value. • **sha1** - Security Hash Algorithm (SHA) algorithm 1 produces a 160-bit hash value. • **sha256** - Security Hash Algorithm (SHA) algorithm 1 produces a 256-bit hash value. • **sha384** - Security Hash Algorithm (SHA) algorithm 1 produces a 384-bit hash value. • **sha512** - The most powerful SHA algorithm that produces a 512-bit hash value. • **null** - No hashing. **NOTE:** For *hash-alg* the value cannot be **null**. So, this is an unsupported, discontinued, and older value.
priority *num*	Tie-breaker value for cases where more than one set of encryption and hashing algorithms are supported by

Parameter	Description
	both VPN gateways. In this case, ACOS selects the group with the highest priority. The priority num value can be 1-10. The highest priority value is 1. The lowest priority value is 10. The configurations for VPN gateways and VPN auto-tunnels each have their own algorithm groups.

Default aes-128-sha1

Mode IKE Gateway mode

interface-management

Description Handles traffic on management interface and only in the shared partition. When the IKE gateway is configured with a management interface, the local IP of the IKE gateway must be the IP address on the management interface. The management traffic is sent to the IKE gateway peer IP address over the IPsec tunnel. The maximum IPsec gateway is 8, and the maximum IPsec tunnel is 8.

Syntax

```
[no] interface-management
```

Default 1

Mode IKE Gateway mode

Usage Indicates that the IKE gateway is using management interface.

ike-version

Description Choose the IKE protocol version and mode to negotiate SAs for the IPsec sessions and specify the encapsulation mode to be used for IKE v1 during generation of the secret shared keys and private keys. This option is ignored if IKE v2 is used.

Syntax

```
[no] ike-version {v1 (main | aggressive)| v2}
```

Parameter	Description
v1	Choose the IKE v1 key exchange specifications.

Parameter	Description
	• **main** - Negotiate Main mode (Default). This option is more secure but uses more packets. • **aggressive** - Negotiate Aggressive mode. This option is less secure but uses fewer packets.
v2	Choose the IKE v2 key exchange specifications.

Default IKE v2

Mode IKE Gateway mode

Example The following example shows the usage of the **ike-version** command:

```
ACOS(config-ike-gateway:jumbo)#ike-version ?
  v1  IKEv1 key exchange
  v2  IKEv2 key exchange
ACOS(config-ike-gateway:jumbo)#ike-version v2 ?
  <cr>
ACOS(config-ike-gateway:jumbo)#ike-version v1 mode ?
  main        Negotiate Main mode (Default)
  aggressive  Negotiate Aggressive mode
```

key

Description Configure the private key used for certificate-based authentication. To import a certificate, use the **import cert** command.

Syntax

```
[no] key PRIVATE-KEY passphrase
```

Parameter	Description
passphrase	Uses the string you enter as the key. The same key value must be configured on the local VPN gateway in ACOS and on the remote gateway, 1-255 characters. The passphrase is encrypted.

Default No private key is specified

Mode IKE Gateway mode

Usage This option is applicable only for the **auth-method rsa-signature and ecdsa-signature**. To clear the passphrase, use the **key <FILENAME>** command.

lifetime

Description Lifetime is the maximum number of seconds an IKE SA can remain in effect. After the SA ages out, a new IKE SA and child ESP SA are negotiated. Then, the old SA and any child SAs for ESP based on the old IKE SA are deleted.

Syntax

```
[no] lifetime seconds
```

Parameter	Description
seconds	IKE SA age in seconds. You can specify 300-86400 *seconds*.

Default 86400 seconds (24 hours)

Mode IKE Gateway mode

local-address

Description Local address is the IP address of the local VPN gateway (or IKE gateway). For ACOS to send and receive traffic for the gateway, specify an IP address that belongs to (is configured on) the ACOS device.

Syntax

```
[no] local-address ip | ipv6
```

Parameter	Description
ip	Valid IPv4 address.
ipv6	Valid IPv6 address.

Mode IKE Gateway mode

local-cert

Description Name of the certificate the ACOS device should present to the remote gateway during IKE negotiation. The certificate must be imported for

the VPN gateway to access the certificate. SCEP-enrolled certificates are supported. To import the **rsa** or **ecdsa** certificate, use the **import cert** command.

Syntax `[no] local-cert filename`

Parameter	Description
filename	Specify the certificate file name, 1-255 characters.

Default N/A

Mode IKE Gateway mode

local-id

Description Local ID is the ID value of the gateway for IKE phase 1.

Syntax `[no] local-id string`

Parameter	Description
string	Specify a valid fully-qualified domain name (FQDN) string, 1-128 characters.

Default N/A

Mode IKE Gateway mode

nat-traversal

Description Enables NAT traversal. This feature allows ACOS to establish a VPN connection with an end point that is on the other side of a NAT device. When this option is enabled, ACOS encapsulates ESP traffic inside UDP packets before sending them to the peer VPN gateway. The source port for the packets is UDP 4500 (based on RFC 5996). The destination UDP port number is the same as the encapsulated packet's destination port number.

Syntax `[no] nat-traversal`

Default Disabled

Mode IKE Gateway mode

remote-address

Description Remote address is the DNS name or IP address of the peer VPN gateway. For VPN to work between the local VPN gateway in ACOS and the remote gateway, the ACOS device must have an IP route through which traffic can reach the remote gateway. Ensure the remote address is pingable from the local address.

NOTE: Dynamic `remote-address` and `remote-id` for the IPsec VPN peers are supported only with IKEv2. If the `remote-address` or `remote-id` is dynamic, define only the `local-address` or `local-id` in the configuration. The remote device must initiate the tunnel as the local device will not know the remote device's address.

Syntax

```
[no] remote-address {dns domain-name | ip ipaddr | ipv6 ipv6addr}
```

Parameter	Description
domain-name	Remote IP based on the domain name.
ipaddr	Valid IPv4 address.
ipv6addr	Valid IPv6 address.

Default N/A

Mode IKE Gateway mode

remote-ca-cert

Description Name of the CA certificate that signs the server certificate presented by the remote gateway. ACOS (the local IKE gateway) uses the CA certificate as a way to validate the remote gateway's server certificate. If the remote gateway's server certificate was signed by the CA certificate imported onto the ACOS device, and you trust the source of that CA certificate, then ACOS trusts the remote gateway's server's certificate. This option is applicable only with auth-method rsa-signature or ecdsa-signature. You must import the remote VPN

gateway's CA-signed certificate onto the ACOS device (the local VPN gateway); use the import cert command.

Syntax

```
[no] remote-ca-cert filename
```

Parameter	Description
filename	Specify the certificate file name, 1-127 characters.

Default N/A

Mode IKE Gateway mode

remote-id

Description Remote ID is the ID value of the peer gateway for IKE phase 1.

NOTE: Dynamic `remote-address` and `remote-id` for the IPsec VPN peers are supported only with IKEv2. If the `remote-address` or `remote-id` is dynamic, define only the `local-address` or `local-id` in the configuration. The remote device must initiate the tunnel as the local device will not know the remote device's address.

Syntax

```
[no] remote-id string
```

Parameter	Description
string	Specify a valid FQDN string, 1-128 characters.

Default N/A

Mode IKE Gateway mode

vrid

Description Selects the VRID to which the gateway is assigned for redundancy.

Syntax

```
[no] vrid {default | num}
```

Parameter	Description
default	Default VRRP-A vrid.

Parameter	Description
	NOTE: For the **vrid** command, the **default** option is not applicable and available now.
num	Specify the VRID (0-31). If configuring a VRID in an L3V partition, use 0-7.

Default Disabled

Mode IKE Gateway mode

radius-server

Description Configures the client's radius server IP address when the client connects to the server.

Syntax

```
[no] radius-server {pri| sec} name
```

Parameter	Description
pri *name*	Primary RADIUS authentication server. It is of 1-63 characters.
sec *name*	Secondary RADIUS authentication server. It is of 1-63 characters.

Default N/A

Mode IKE Gateway mode

Usage This command configures the Radius server for authenticating the client and getting the IP address, netmask, gateway, and other parameters for the configuration payload.

vpn ike-acc-enable

Description Enables IKE acceleration by Cavium Nitrox card.

Syntax

```
[no] vpn ike-acc-enable
```

Default N/A

Mode Global configuration mode

vpn ike-sa timeout

Description Timeout IKE SAs on the system if SAs are in a connecting state for too long.

Syntax

```
[no] vpn ike-sa timeout seconds
```

Parameter	Description
seconds	IKE SA timeout in seconds.

Default 600 seconds

Mode Global configuration mode

vpn ike-stats-global

Description Displays global IKE statistics.

Syntax

```
[no] vpn ike-stats-global
```

Default N/A

Mode Global configuration mode

vpn ipsec

Description Configure an IPsec tunnel. This command changes the CLI to the configuration level for the specified IPsec tunnel.

Syntax

```
[no] vpn ipsec tunnel-name
```

Parameter	Description
tunnel-name	Name of the IPsec tunnel, 1-31 characters.

Default N/A

Mode Global configuration mode

anti-replay-window

Description Number of the IPsec packets for which the ACOS device remembers the IPsec packet sequence numbers. The anti-replay window protects against replay attacks, in which a malicious party sends the IPsec packets containing sequence numbers captured from the session's legitimate traffic.

Syntax

```
[no] anti-replay-window bits
```

Syntax

```
[no] anti-replay-window bits
```

Parameter	Description
bits	You an specify 0, 32, 64, 128, 256, 512, 1024, 2048, 3072, 4096, 8192. Setting the window size to 0 disables anti-replay checking. • 0 - Disable Anti-Replay Window Check • 32 - Window size of 32 • 64 - Window size of 64 • 128 - Window size of 128 • 256 - Window size of 256 • 512 - Window size of 512 • 1024 - Window size of 1024 • 2048 - Window size of 2048 • 3072 - Window size of 3072 • 4096 - Window size of 4096 • 8192 - Window size of 8192

Default N/A

Mode IPsec Tunnel mode

bind

Description Binds a tunnel interface to an IPsec connection.

Syntax

```
[no] bind tunnel num ipaddr
```

Parameter	Description
num	
ipaddr	

Default N/A

Mode IPsec Tunnel mode

crl

Description Configures a certificate revocation list.

Syntax

```
crl {pri | sec} filename
```

Syntax

```
crl {pri | sec} filename
```

Parameter	Description
pri *filename*	Primary CRL File Name or URL (http://www.example.com/ocsp) (only .der filetypes).
sec *filename*	Secondary CRL File Name or URL (http://www.example.com/ocsp) (only .der filetypes).

Default N/A

Mode VPN revocation mode

dh-group

Description Specify the DH group to be used for PFS.

Syntax

```
[no] dh-group group-num
```

Parameter	Description
group-num	• 0 - Diffie-Hellman group 0 (Default) • 1 - Diffie-Hellman group 1 - 768-bits • 2 - Diffie-Hellman group 2 - 1024-bits • 5 - Diffie-Hellman group 5 - 1536-bits • 14 - Diffie-Hellman group 14 - 2048-bits • 15 - Diffie-Hellman group 15 - 3072-bits • 16 - Diffie-Hellman group 16 - 4096-bits • 18 - Diffie-Hellman group 18 - 8192-bits • 19 - Diffie-Hellman group 19 - 256-bit Elliptic Curve • 20 - Diffie-Hellman group 20 - 384-bit Elliptic Curve.

Default 0 (PFS Disabled)

Mode IPsec Tunnel mode

dhcp-server

Description Configures the client's dhcp server IP address when the client connects to the server.

Syntax

```
[no] dhcp-server {pri| sec ip address}
```

Parameter	Description
pri *ip address*	Primary DHCP Server IP Address.
sec *ip address*	Secondary DHCP Server IP Address.

Default N/A

Mode IKE Gateway mode

Usage This command configures the DHCP server, from which the IP address, netmask, gateway, and other parameters for the configuration payload are obtained.

disable

Description Disable the tunnel interface.

Syntax

```
disable
```

Mode IPsec Tunnel Interface mode

Example The following example shows the usage of the *disable* command.

```
ACOS(config)#interface tunnel 1
ACOS(config-if:tunnel:1)#?
  disable    Disable
```

disable-rekey

Description Disables initiating rekey.

Syntax

```
no disable-rekey
```

Default N/A

Mode IKE Gateway mode

Usage This command disables initiating the rekey process. Rekey is the process of creating a new SA to replace an expiring SA before it expires.

domain

Description Specify the domain name for which you want to issue the CA certificate. The CA server will verify whether you control this domain. You can specify 1-64 characters.

Syntax

```
[no] domain
```

Default N/A

Mode ACME certificate mode

enable

Description Enable the tunnel interface.

Syntax

```
enable
```

Mode IPsec Tunnel Interface mode

Example The following example shows how to access the *enable* command.

```
ACOS(config)#interface tunnel 1
ACOS(config-if:tunnel:1)#?
  enable     Enable
```

encryption

Description Specify the encryption algorithm settings for the IPsec. The IPsec tunnel can have up to 4 algorithm groups. During SA negotiation, one of the configured algorithm groups is selected. The options are the same as those supported for IKE gateways. If one of the four algorithm groups are the same for the encryption configuration, then the tunnel sets up. if all differ, tunnel sets down.

Syntax

```
[no] encryption encrypt-alg hash hash-alg {priority num}
```

Parameter	Description
encrypt-alg	Specify the encryption algorithm to be used. • **des** - Data Encryption Standard (DES) is a cryptographic algorithm with a 56-bit key. • **3des** - Triple DES is a more powerful version of DES that uses a 168-bit key. • **aes-128** - Advanced Encryption Standard (AES) is more efficient cryptographic algorithm with a 128-bit key. • **aes-192** - AES algorithm that uses a more powerful 192-bit key. • **aes256** - The most powerful AES algorithm that uses a 256-bit key. • **aes-gcm-128** - Advanced Encryption Standard algorithm Galois/Counter Mode (key size: 128 bits, ICV size: 16 bytes). • **aes-gcm-192** - Advanced Encryption Standard

Parameter	Description
	algorithm Galois/Counter Mode(key size: 192 bits, ICV size: 16 bytes). • **aes-gcm-256** - Advanced Encryption Standard algorithm Galois/Counter Mode (key size: 256 bits, ICV size: 16 bytes). • **null** - No encryption.
hash-alg	Specify the hashing algorithm to be used. • **md5** - Message Digest Algorithm 5 (MD5) is a hashing algorithm that produces a 128-bit hash value. • **sha1** - Security Hash Algorithm (SHA) algorithm 1 produces a 160-bit hash value. • **sha256** - Security Hash Algorithm (SHA) algorithm 1 produces a 256-bit hash value. • **sha384** - Security Hash Algorithm (SHA) algorithm 1 produces a 384-bit hash value. • **sha512** - The most powerful SHA algorithm that produces a 512-bit hash value. • **null** - No encryption.

Default aes-128-sha1

Mode IPsec Tunnel mode

Example

```
(config-ipsec:1)#encryption null hash ?
md5     MD5 Dessage-Digest Algorithm
sha1    Secure Hash Algorithm 1
sha256  Secure Hash Algorithm 256
sha384  Secure Hash Algorithm 384
sha512  Secure Hash Algorithm 512
null    No hash algorithm
(config-ipsec:1)#
```

enroll

Description Initiates enrollment of device with the CA.

Syntax

```
[no] enroll
```

Default Disabled

Mode CMP certificate mode

force

Description Enables to do the enrollment again. In the ACME certificate, the **force** option will be automatically enabled for the renewal.

Syntax

```
[no] force
```

Default N/A

Mode ACME certificate mode

fragment-size

Description Enables the IKE message fragment and sets the fragment size.

Syntax

```
[no] fragment-size fragment-size
```

Parameter	Description
fragment-size	Specify the fragment size. The value can be 576 – 1280 bytes.

Default N/A

Mode IKE Gateway mode

Usage This command fragments large IKE messages into a series of smaller messages when the digital certificates are used for IKE authentication and allows establishing an IPsec tunnel.

Example The following configuration example sets the fragment size to 578.

```
ACOS(config)#vpn ike-gateway small
ACOS(config-ike-gateway:small)#fragment-size 578
```

ike-gateway

Description IKE gateway is the name of the VPN gateway that is used for tunnel connections.

Syntax

```
[no] ike-gateway gateway-name
```

Parameter	Description
gateway-name	Name of the gateway for the IPsec SA, 1-31 characters.

Default N/A

Mode IPsec Tunnel mode

lifebytes

Description Maximum number of megabytes (MB) of data that can be transferred using a given SA.Setting this option to 0 disables aging based on bytes.

Syntax

```
[no] lifebytes Mb
```

Parameter	Description
Mb	The IPsec SA age in megabytes. You can specify <0-8000000> megabytes.

Default 0 (unlimited)

Mode IPsec Tunnel mode

lifetime

Description Maximum number of seconds an IPsec SA can remain in effect.

Syntax

```
[no] lifetime seconds
```

Parameter	Description
seconds	The IPsec SA age in seconds.You can specify 300-28800 *seconds*.

Default 28800 seconds (8 hours)

Mode IPsec Tunnel mode

mode

Description Mode specifies the encapsulation mode for the IPsec traffic. Only tunnel mode is supported. In the tunnel mode, the client packet is encrypted and encapsulated in an IP packet.

Syntax

```
[no] mode tunnel
```

Default Tunnel mode

Mode IPsec Tunnel mode

mtu

Description Change the Maximum Transmission Unit (MTU) for a Tunnel interface.

Syntax

```
mtu bytes
```

Parameter	Description
bytes	Largest packet size that can be forwarded out the interface without fragmentation. You can specify between 68 to 1200 bytes.

Default 1500

Mode IPsec Tunnel Interface mode

Usage If the ACOS device needs to forward a packet that is larger than the MTU of the ACOS egress interface to the next hop, but the Do Not Fragment bit is set in the packet, the ACOS device drops the packet and sends an ICMP Destination Unreachable code 4 (Fragmentation required, and DF set) message to the sender. If the Do Not Fragment bit is not set, the ACOS device silently drops the packet.

Example The following example shows how to access the *mtu* command.

```
ACOS#conf
ACOS(config)#interface tunnel 1
ACOS(config-if:tunnel:1)#
```

```
  mtu        Interface mtu
```

proto

Description Specify the protocol used to encrypt traffic on the tunnel. The current release supports ESP.

Syntax

```
[no] proto esp
```

Default ESP

Mode IPsec Tunnel mode

sequence-number-disable

Description Do not use incremental sequence numbers in the ESP header.

Syntax

```
sequence-number-disable
```

Default 1

Mode IPsec Tunnel mode

speed

Description To configure speed on the tunnel interface in Gbit/sec.

Syntax

```
speed <speed in Gbit/Sec>
```

Default 10 Gbps

Mode IPsec Tunnel Interface mode

Usage The following example shows how to configure speed on the tunnel interface.

```
ACOS#conf
ACOS(config)#interface tunnel 1
ACOS(config-if:tunnel:1)#speed ?
<1-200> Speed in Gbit/Sec (Default 10 Gbps)
```

traffic-selector

Description Specify the networks, protocols, and ports that pass through the IPsec tunnel.

Syntax

```
[no] traffic-selector [ipv4 local ipaddr {netmask | /mask-length} remote ipaddr {netmask | /mask-length}]
```

Parameter	Description
local *ipaddr*	Specify the local traffic selector IPv4 address.
local *netmask*	Specify the IPv4 address network mask.
local *port*	Specify the port number.
local *protocol*	Specify the IP Protocol Number, 0-255.
remote *ipaddr*	Specify the IP address of the interface that terminates the tunnel.
remote *netmask*	Specify the IPv4 Address Network Mask.
remote *port*	Specify the UDP port number.
remote *protocol*	Specify the IP protocol number, 0-255.
ipv6ddr	Specify the local or remote traffic selector IPv6 address.

Syntax

```
[ipv6 ipv6addr]
```

Default N/A

Mode IPsec Tunnel mode

up

Description Initiates SA negotiation to bring up an IPsec connection on the tunnel.

Syntax

```
(config-ipsec:1)#up?
up Initiates SA negotiation to bring the IPsec connection up
(config-ipsec:1)#no ?
anti-replay-window Anti-replay window size
bind Binds tunnel interface to the IPsec connection
dh-group DH Group for Perfect Forward Secrecy
encryption Encryption algorithm for an IPsec transform
ike-gateway Gateway to use for IPsec SA
lifebytes IPsec SA age in megabytes (0 indicates unlimited
```

```
bytes)
lifetime IPsec SA age in seconds
mode Encapsulation mode (tunnel or transport)
proto Encapsulation Protocol
sampling-enable Enable baselining
sequence-number-disable Do not use incremental sequence number
in the ESP header
traffic-selector Traffic Selectors define the set of traffic
for the SA
user-tag Customized tag
(config-ipsec:1)#no
```

Default Disabled

Mode IPsec Tunnel mode

vpn ipsec-cipher-check

Description For a secure environment, the following conditions should be fulfilled to ensure that weaker ciphers are not used:

- IKE SA should not use weaker cipher than IPSec SA.
- Both IKE SA and IPsec SA should not use weaker ciphers such as Des/3DES/MD5.

The command enables the function where the IPsec tunnel is not established if the conditions mentioned above are not fulfilled.

NOTE: This command can be configured under shared partition.

Syntax

```
[no] vpn ipsec-cipher-check
```

Default Disabled

Mode Global configuration mode

Usage If the conditions mentioned in the description above are not fulfilled, a log is created, a message is sent to the peer site, and the IPsec tunnel is not established.

vpn ipsec-group

Description Grouping IPsec tunnels. It can have one active tunnel and one or more backup tunnels.

Syntax

```
[no] vpn ipsec-group group-name
```

Parameter	Description
group-name	Name of the IPsec tunnel group. It can be 1-31 characters.

Default N/A

Mode Global configuration mode

Usage This command forms a group of tunnels under the specified group name (group-name).

Example The following example creates an IPsec tunnel named a1 and adds a group named group1.

```
ACOS(config)#vpn ipsec a1
ACOS(config-ipsec:a1)#lifetime 300
ACOS(config-ipsec:a1)#bind tunnel 1 12.12.12.1
ACOS(config-ipsec:a1)#ike-gateway a1
ACOS(config-ipsec:a1)#exit
ACOS(config)#vpn ipsec-group group1
```

ipsec

Description Configures group members for the ipsec-group.

Syntax

```
ipsec <ipsec-name> priority <pri-value>
```

Parameter	Description
ipsec *ipsec-name*	Specify one of the tunnels as a group member.
priority *pri-value*	Specify the priority for the group member. The priority can be 1-10.

Parameter	Description
	The highest priority value is the active tunnel.

Default N/A

Mode IPsec Group mode

Usage This command helps to add group members to the IPsec Group and set the priority. The tunnel with the highest priority is the primary tunnel (active) and traffic flows through it.
If the priority of the backup tunnel is changed to a priority higher than the primary tunnel, the backup tunnel becomes the primary tunnel and traffic flows through it.

Example The following example adds a group member named a1 and sets the priority to 9.

```
ACOS(config)#vpn ipsec-group group1
ACOS(config-ipsec-group:group1)# ipsec a1 priority 9
```

vpn jumbo-fragment

Description Enable support for IKE jumbo frame fragmentation.

Syntax `[no] vpn jumbo-fragment`

Default Disabled

Mode Global configuration mode

vpn nat-traversal-flow-affinity

Description Chooses the IPsec UDP source port based on port of inner flow.

Syntax `[no] vpn nat-traversal-flow-affinity`

Default Disabled

Mode Global configuration mode

vpn revocation

Description Configure the IPsec VPN revocation settings. This command changes the CLI to the configuration level for the VPN Revocation Mode.

Syntax

```
[no] vpn revocation revocation-name
```

Parameter	Description
revocation-name	Name of the VPN revocation, 1-31 characters.

Default N/A

Mode Global configuration mode

ca

Description Revokes a VPN CA certificate.

Syntax

```
ca filename
```

Parameter	Description
filename	Specify the certificate authority file name, <1-255>.

Default N/A

Mode VPN revocation mode

ocsp

Description Revokes certificates being managed by Online Certificate Status Protocol (OCSP) server.

Syntax

```
ocsp {pri | sec} server
```

Parameter	Description
pri *server*	Primary OCSP authentication server, 1-31 characters.
sec *server*	Secondary OCSP authentication server, 1-31 characters.

Default N/A

Mode VPN revocation mode

vpn signature-authentication

Description Enables using different hash algorithms for signature authentication in Internet Key Exchange version 2 (IKEv2).

Syntax

```
[no] vpn signature-authentication
```

Default Disabled

Mode Global configuration mode

Usage Signature Authentication in IKEv2 increases the capability to use stronger hash algorithms while generating authentication payloads during an IKEv2 negotiation.

Example The following command enables using different hash algorithms for signature authentication in IKEv2:

```
ACOS(config)#vpn signature-authentication
```

The output of the `show vpn` command displays the configuration status of signature authentication.

vpn stateful-mode

Description Configure the ACOS device to setup sessions for the IPsec traffic.

Syntax

```
[no] vpn stateful-mode
```

Default Disabled

Mode Global configuration mode

vpn tcp-mss-adjust-disable

Description Disable TCP MSS adjustment in SYN packet to avoid fragmentation overhead.

Syntax

```
[no] vpn tcp-mss-adjust-disable
```

Default Disabled

Mode Global configuration mode

Show Commands

clear pki

Description Clears the PKI certificate log and debug information.

Syntax

```
clear pki {acme-cert| scep-cert} logname
```

Parameter	Description
acme-cert	Clears the ACME certificate related information.
scep-cert	Clears the SCEP certificate related information.
log *name*	Clears the ACME or SCEP certificate enrollment log and debug information.

Mode Configuration mode

Example The following command clears the ACME log.

```
ACOS(config)# clear pki acme-cert log test
```

clear vpn crl

Description Clear VPN Revocation information.

Syntax `clear vpn crl`

Default N/A

Mode Global configuration mode

clear vpn ike-sa

Description Clears IKE SAs for the specified gateway.

Syntax `clear vpn ike-sa {gateway-name | all-partitions}`

Parameter	Description
gateway-name	Specify the IKE gateway name.
all-partitions	Clear IKE SA information for all partitions. Without this option, SA information is cleared only for the partition from which you enter the command.

Default N/A

Mode Global configuration mode

clear vpn ike-stats

Description Clear VPN IKE statistics.

Syntax `clear vpn ike-stats {gateway-name | all-partitions}`

Parameter	Description
gateway-name	Specify the IKE gateway name.

Parameter	Description
all-partitions	Clear IKE statistics information for all partitions. Without this option, IKE statistics are cleared only for the partition from which you enter the command.

Default N/A

Mode Global configuration mode

clear vpn ike-stats-global

Description Clear VPN IKE global statistics.

Syntax `clear vpn ike-stats-global {all-partitions}`

Parameter	Description
all-partitions	Clear IKE statistics information for all partitions. Without this option, IKE statistics are cleared only for the partition from which you enter the command.

Default N/A

Mode Global configuration mode

clear vpn ipsec-group

Description Clears all the SAs associated with the group.

Syntax `clear vpn ipsec-group {group-name | all-partitions}`

Parameter	Description
group-name	Specify the group name.
all-partitions	Clears the SAs of all the groups in all partitions.

Default N/A

Mode Global configuration mode

clear vpn ipsec-sa

Description This command brings the specified IPsec tunnel down. It may take a few seconds for this command to execute.

Syntax

```
clear vpn ipsec-sa {tunnel-name | all-partitions}
```

Parameter	Description
tunnel-name	Specify the IPsec tunnel name.
all-partitions	Clear the IPsec SA information for all partitions. Without this option, the IPsec SA are cleared only for the partition from which you enter the command.

Default N/A

Mode Global configuration mode

clear vpn log

Description Clear VPN log and debug information.

Syntax

```
clear vpn log
```

Default N/A

Mode Global configuration mode

clear vpn ocsp

Description Clear OCSP information.

Syntax

```
clear vpn ocsp
```

Default N/A

Mode Global configuration mode

debug monitor

Description Show all currently active debug output on terminal.

Syntax

```
debug monitor
```

Default N/A

Mode Configuration Mode

Example Enable debug tunnel and debug monitor, then trigger the IPsec VPN tunnel.

```
ACOS#debug tunnel
ACOS#debug monitor
```

debug packet

Description Debug packets.

Syntax

```
debug packet {count | detail | interface | l3-protocol | l4-protocol}
```

Parameter	Description
count	The count of the maximum packets to capture. Default is 3000.
detail	Print packet content.
interface	Specify the ethernet interface number to debug.
l3-protocol	Layer 3 protocol (ARP, IP, IPv6, IPv6 neighbor/Router).
l4-protocol	Layer 4 protocol (ICMP, ICMPv6, TCP, UDP).

Default N/A

Mode Enable Mode

Example Enable debug tunnel, debug packet and debug monitor, then trigger the IPsec VPN tunnel.

```
ACOS#debug tunnel
ACOS#debug packet
ACOS#debug monitor
```

debug tunnel

Description Debug a VPN tunnel.

Syntax **debug tunnel**

Default N/A

Mode Enable Mode

debug vpn level

Description Debug an IPsec VPN tunnel at each level.

Syntax **debug vpn level** {*1* | *2* | *3* | *4*}

Parameter	Description
1	Basic Packet Negotiation.
2	Diagnose Problems.
3	Raw Binary Blobs.
4	Sensitive Data (Private Keys)

Default N/A

Mode Enable Mode

show counters-rate

Description Show the bandwidth rate statistics for the IPsec tunnels.

Syntax `show counters-rate vpn ipsec tunnel-name`

Default N/A

Mode IPsec Tunnel mode

Usage For use with the vpn ipsec command.

Example The following example scenario includes enabling sampling on the ACOS device, which is disabled by default, and then showing the bandwidth utilized by the tunnel. In this example, client1 is the SFTP server and client2 is the SFTP client. The output below includes the overall statistics of encrypted traffic when client2 downloads a file from client1. The unit of the rate depends on the unit of the counter per second. For example, if the counter is bytes, the rate is bytes per second.

```
ACOS#config
ACOS(config)#vpn ipsec tunnel-name
ACOS(config-ipsec:microsoft-tunnel)#sampling-enable all
ACOS(config-ipsec:microsoft-tunnel)#show counters-rate vpn
ipsec tunnel-name
counter_name            1sec_rate   5sec_rate    10sec_rate     30sec_
rate
Encrypted Packets       2562        2372         2472   3185
Decrypted Packets       1357        1259         1321   1165
Anti-Replay Failure     0           0            0          0
Rekey Times             0           0            0          0
Inactive Error          0           0            0          0
Encryption Error        0           0            0          0
Pad Check Error         0           0            0          0
Packets Sanity Error    0           0            0          0
ICV Check Error         0           0            0          0
Lifetime Lifebytes Error0           0            0            0
Encrypted Bytes         3352960     3108451      32402204225355
Decrypted Bytes         83608           77574    81724 74959
Pre-frag Success        2348            2177     2272           3038
Pre-frag Error          0            0           0          0
CAVIUM Encrypted Bytes  0            0           0            0
CAVIUM Decrypted Bytes  0            0           0            0
CAVIUM Encrypted Packets0            0           0            0
```

```
CAVIUM Decrypted Packets0              0              0              0
```

show counters vpn ike-gateway [NAME]

Description Shows the IKE gateway settings.

For the Multi-PU platforms, the `show counters vpn ike-gateway <name>` displays the counters on PU1 and zero counter on PU2.

Syntax

```
show counters vpn ike-gateway
```

Default N/A

Mode All

Example The following command shows the counters for vpn ike-gateway psk (preshared key):

```
ACOS#show counters vpn ike-gateway psk
Initiate Rekey                          8
Respond Rekey                           0
Child SA Rekey                          9
Incoming Invalid                        0
Incoming Invalid SPI                    0
Incoming Init Request                   0
Incoming Init Response                  4
Outgoing Init Request                   4
Outgoing Init Response                  0
Incoming Auth Request                   0
Incoming Auth Response                  4
Outgoing Auth Request                   4
Outgoing Auth Response                  0
Incoming Create Child Request           0
Incoming Create Child Response          17
Outgoing Create Child Request           17
Outgoing Create Child Response          0
Incoming Info Request                   14
Incoming Info Response                  28
Outgoing Info Request                   28
Outgoing Info Response                  14
Incoming ID Protection Request          0
```

```
Incoming ID Protection Response          0
Outgoing ID Protection Request           0
Outgoing ID Protection Response          0
Incoming Auth Only Request               0
Incoming Auth Only Response              0
Outgoing Auth Only Request               0
Outgoing Auth Only Response              0
Incoming Aggressive Request              0
Incoming Aggressive Response             0
Outgoing Aggressive Request              0
Outgoing Aggressive Response             0
Incoming Info Request                    0
Incoming Info Response                   0
Outgoing Info Request                    0
Outgoing Info Response                   0
Incoming Transaction Request             0
Incoming Transaction Response            0
Outgoing Transaction Request             0
Outgoing Transaction Response            0
Incoming Quick Mode Request              0
Incoming Quick Mode Response             0
Outgoing Quick Mode Request              0
Outgoing Quick Mode Response             0
Incoming New Group Mode Request          0
Incoming New Group Mode Response         0
Outgoing New Group Mode Request          0
Outgoing New Group Mode Response         0
Invalid SPI for Child SAs                0
Invalid SPI for Child SAs                0
IKE version                              2
```

show counters vpn ipsec [NAME]

Description Shows the IPsec settings.

For the Multi-PU platforms, the `show counters vpn ipsec <name>` displays the aggregated counters from PU1 and PU2 on PU1. However, on PU2, this command displays only the counters from PU2.

Syntax

```
show counters vpn ipsec
```

Default N/A

Mode All

Example The following command shows the counters for vpn ipsec psk (preshared key):

```
ACOS#show counters vpn ipsec psk
Encrypted Packets                          0
Decrypted Packets                          0
Anti-Replay Failure                        0
Rekey Times                                0
Inactive Error                             0
Encryption Error                           0
Pad Check Error                            0
Packets Sanity Error                       0
ICV Check Error                            0
Lifetime Lifebytes Error                   0
Encrypted Bytes                            0
Decrypted Bytes                            0
Pre-frag Success                           0
Pre-frag Error                             0
CAVIUM Encrypted Bytes                     0
CAVIUM Decrypted Bytes                     0
CAVIUM Encrypted Packets                   0
CAVIUM Decrypted Packets                   0
QAT Encrypted Bytes                        480
QAT Decrypted Bytes                        480
QAT Encrypted Packets                      5
QAT Decrypted Packets                      5
Packet dropped: Tunnel Interface Down      0
Packet dropped: Failed in prepare to send  0
Packet dropped: No next hop                0
Packet dropped: Invalid tunnel ID          0
Packet dropped: No tunnel found            0
Packet dropped: Failed to send             0
Frag-after-encap Fragment Generated        0
Fragment Received                          0
Sequence Number                            5
Sequence Number Rollover                   0
Next Header Check Error                    0
```

show hardware

Description View the hardware available. If you do not see FTA, hardware acceleration is not possible and slower response time could be experienced.

Syntax `show hardware`

Default N/A

Mode All

show vpn

Description Displays the summary of VPN configuration and Security Association (SA) information.

For the Multi-PU platforms, the `show vpn` output is displayed only on PU1.

Syntax `show vpn`

Default N/A

Mode All

Example The following example shows the sample output for the **`show vpn`** command:

```
ACOS#show vpn
IKE Gateway total:    1
IPsec total:          1
IKE SA total:         0
IPsec SA total:       0
IPsec mode: software
IPsec passthrough traffic
CPU 0 processed 0 packets
CPU 1 processed 0 packets
```

Example The following example shows the sample output of the `show vpn` command, which displays the configuration status of signature authentication (Enabled or Disabled).

```
ACOS(config)#show vpn
Partition shared
IKE Gateway total:   5
IPsec total:         5
IKE SA total:        0
IPsec SA total:      0
IPsec stateless mode
IPsec encryption mode: Software
IPsec passthrough traffic
HA standby drop:          0
Signature Authentication: Enabled
```

show vpn all-partitions

Description Display the summary of VPN configuration information for all partitions on the ACOS device. If you omit the all-partitions option, VPN information for the current partition is shown.

For the Multi-PU platforms, the `show vpn all-partitions` output is displayed only on PU1.

Syntax

```
show vpn all-partitions
```

Default N/A

Mode All

Example The following example shows the sample output for the **`show vpn all-partitions`** command:

```
ACOS#show vpn all-partitions
Partition shared
IKE Gateway total:   0
IPsec total:         0
IKE SA total:        0
IPsec SA total:      0
IPsec mode: software
```

```
IPsec passthrough traffic
CPU 0 processed 0 packets
```

show vpn partition <NAME>

Description Displays the summary of per-partition configuration.

For the Multi-PU platforms, the `show vpn partition <name>` output is displayed only on PU1.

Syntax **`show vpn partition`** {*name* | **`shared`**}

Default N/A

Mode All

Example The following example shows the sample output for the **`show vpn partition`** command:

```
ACOS#show vpn partitions s4
Partition shared
IKE Gateway total:    0
IPsec total:          0
IKE SA total:         0
IPsec SA total:       0
IPsec mode: software
IPsec passthrough traffic
CPU 0 processed 0 packets
```

show vpn crl

Description Display VPN cached crl certificates.

Syntax **`show vpn crl`**

Default N/A

Mode All

show vpn default

Description Display the default VPN configuration settings in the ACOS release running on your device.

Syntax

```
show vpn default
```

Default N/A

Mode All

Example The following command shows the default configuration settings for VPN:

```
ACOS#show vpn default
IKE Gateway:
IKE version: v2
           Mode:                main
           DH group:            1
           Auth method:         preshare-key
           Encryption:          aes-128
           Hash:                sha1
           Priority:            5
           Lifetime:            86400 (seconds)
           NAT traversal:       Disable
           Local address ip:    0.0.0.0
           Remote address ip:   0.0.0.0
           DPD interval:        0 (seconds)
IPsec:
           Mode:                tunnel
           Protocol:            esp
           DH group:            0
           Encryption:          aes-128
           Hash:                sha1
           Priority:            5
           Lifetime:            28800 (seconds)
           Lifebytes:           0 (MB)
           Traffic selector:    manual
           Local subnet:        0.0.0.0/0
           Local Port:          0
           Local Protocol:      0
```

```
            Remote subnet:        0.0.0.0/0
            Remote Port:          0
            Remote Protocol:      0
            Anti-replay window:   0
```

show vpn ike-sa

Description Shows the IKE SA information.

For the Multi-PU platforms, the `show vpn ike-sa <name>` output is displayed only on PU1.

Syntax **`show vpn ike-sa`** {*gateway-name* | **`all-partitions`**}

Parameter	Description
gateway-name	Specify the IKE gateway name.
all-partitions	Shows IKE SA information for all partitions. Without this option, SA information is listed only for the partition from which you enter the command.

Default N/A

Mode All

Example The following command shows the summary of IKE SA information for the current partition:

```
ACOS#show vpn ike-sa

Name      Local/Peer IP  Enc/Hash  Lifetime  Status
-------------------------------------------------------
scep      192.168.38.1   3des        85944s  Established
          192.168.38.2   md5
pkitest   192.10.10.10   3des        85110s  Established
          192.20.20.20   md5
56        193.168.40.1   3des        85092s  Established
          193.168.40.6   md5
-------------------------------------------------------
Total: 3
```

Example The following command shows the summary of IKE SA information for the gateway named v4.

```
ACOS(config)#show vpn ike-sa v4
Gateway Name:  v4
Initiator SPI: 0x1fb2b2dd93348e21       Responder SPI:
0x00082cc628439507
Local IP:      3001::1:10               Remote IP: 3001::1:11
Local ID:      C=IN, ST=MH, L=PNQ, O=A10, OU=QA, CN=AX1-...
Remote ID:     C=IN, ST=MH, L=PNQ, O=A10, OU=QA, CN=AX2-...
Encryption:    aes-256                  Hash:  sha512
Lifetime:      85069s                   Auth-method:  rsa-
signature
DH group:                    18         NAT-T:    disabled
Fragment message generated:  1          Fragment message
received: 1
Fragmentation error:         0          Fragment-reassemble-
error: 0
Status:                      Established
```

Example The following command shows the hash algorithm used to sign authentication payloads in the Auth-method field.

```
ACOS(config-ipsec:a1)#show vpn ike-sa a1
Gateway Name:  a1
Initiator SPI: 0x89dcce2974dcdcc2    Responder SPI:
0x1cc2d9666fc4c40e
Local IP:      19.19.19.2            Remote IP:
19.19.19.3
Local ID:      C=US, ST=CA, L=SJ, O=A10, OU=Engineering,...
Remote ID:     C=US, ST=CA, L=SJ, O=A10, OU=Engineering,...
Encryption:    aes-128                Hash:     sha1
Lifetime:      86384s                 Auth-method: ecdsa-
signature (sha256)
DH group:      1                      NAT-T:     disabled
Fragment message generated:  0        Fragment message
received:   0
Fragmentation error:         0        Fragment-reassemble-
error:   0
Status:                      Established
```

show vpn ike-sa-brief <NAME>

Description Shows IKE SAs for a given IKE Gateway Config.

For the Multi-PU platforms, the `show vpn ike-sa-brief <name>` output is displayed only on PU1.

Syntax `show vpn ike-sa-brief {gateway-name}`

Default N/A

Mode All

Example The following command shows the summary of IKE SA:

```
AX3200-12-186#show vpn ike-sa site

Gateway Name:  site
Initiator SPI: 0xb9ce137bf3559519
Responder SPI: 0x968119a4bc390331
Local IP:      8.8.8.186
Remote IP:     8.8.8.128
Local ID:      tuy.site
Remote ID:     tuy.client
Encryption:    aes-128                                  Hash:
         sha256
Lifetime:      358s                                     Auth-
method:   preshare-key
DH group:      2                                        NAT-
T:         disabled
Status:        Established

Gateway Name:  site
Initiator SPI: 0x02a6590d42215352
Responder SPI: 0x953c38b91b1e0880
Local IP:      8.8.8.186
Remote IP:     8.8.8.124
Local ID:      tuy.site
Remote ID:     tuy.124.client
Encryption:    aes-128                                  Hash:
         sha256
```

```
Lifetime:       202s                                    Auth-
method:    preshare-key
DH group:       2                                       NAT-
T:          disabled
Status:         Established
```

show vpn ike-stats

Description Displays IKE statistics.

For the Multi-PU platforms, the `show vpn ike-stats` output is displayed only on PU1.

Syntax

```
show vpn ike stats {all partitions| gateway-name}
```

Parameter	Description
all-partitions	VPN configuration summary of all partitions.
gateway-name	Specify the IKE-gateway name, 1-31.

Default N/A

Mode All

Example Add some statistics for VPN IKE. With these statistics, A10 Networks can get more information of the IKE and make trouble shooting easy:

```
ACOS#show vpn ike-stats
Gateway: 38                             Respond Rekey:0
Initiate Rekey:0                        Incoming Init Request:0
Child SA Rekey:0                        Incoming Init Response:1
Outgoing Init Request:1                 Incoming Auth Request:0
Outgoing Init Response:0                Incoming Auth Response:0
Outgoing Auth Request:0                 Incoming Create Child
Request:0
Outgoing Auth Response:0                Incoming Create Child
Response:0
Outgoing Create Child Request:0         Incoming Info Request:1
Outgoing Create Child Response:0        Incoming Info Response:0
Outgoing Info Request:0                 Incoming Invalid SPI:0
Outgoing Info Response:1
```

```
Incoming Invalid:0
Gateway: 39                              Respond Rekey:0
Initiate Rekey:0                         Incoming Init Request:0

Child SA Rekey:0                         Incoming Init Response:0
Outgoing Init Request:0                  Incoming Auth Request:0
Outgoing Init Response:0                 Incoming Auth Response:0
Outgoing Auth Request:0                  Incoming Create Child
Request:0
Outgoing Auth Response:0                 Incoming Create Child
Response:0
Outgoing Create Child Request:0          Incoming Info Request:0
Outgoing Create Child Response:0         Incoming Info Response:0
Outgoing Info Request:0                  Incoming Invalid SPI:0
Outgoing Info Response:0
Incoming Invalid:0
Gateway: 40
Initiate Rekey:0
Child SA Rekey:0
```

show vpn ike-stats-global

Description Displays global IKE statistics.

For the Multi-PU platforms, the `show vpn ike-stats-global` output is displayed only on PU1.

Syntax

```
show vpn ike-stats-global {partition | all-partitions}
```

Parameter	Description
partition	VPN configuration summary per partition.
all-partitions	VPN configuration summary of all partitions.

Default N/A

Mode All

Example The output of "`show vpn ike-stats-global`" includes the overall statistics of IKE gateways on current partition:

```
(config-ipsec:1)#sh vpn ipsec-sa ?
  WORD<length:1-31>  IPsec SA name
  all-partitions     All partition configurations
  partition          Per-partition configurations
  |                  Output modifiers
  <cr>

ACOS#show vpn ike-stats-global
         IKE version 1 Statistics
  Outgoing ID Protection Request: 0         Incoming ID
Protection Request: 0
 Outgoing ID Protection Response: 0        Incoming ID
Protection Response: 0
      Outgoing Auth Only Request: 0             Incoming Auth
Only Request: 0
     Outgoing Auth Only Response: 0            Incoming Auth
Only Response: 0
     Outgoing Aggressive Request: 0            Incoming
Aggressive Request: 0
    Outgoing Aggressive Response: 0           Incoming
Aggressive Response: 0
           Outgoing Info Request: 0                  Incoming
Info Request: 0
          Outgoing Info Response: 0                 Incoming
Info Response: 0
    Outgoing Transaction Request: 0           Incoming
Transaction Request: 0
   Outgoing Transaction Response: 0          Incoming
Transaction Response: 0
     Outgoing Quick Mode Request: 0            Incoming Quick
Mode Request: 0
    Outgoing Quick Mode Response: 0           Incoming Quick
Mode Response: 0
 Outgoing New Group Mode Request: 0        Incoming New Group
Mode Request: 0
Outgoing New Group Mode Response: 0       Incoming New Group
Mode Response: 0

         IKE version 2 Statistics
```

```
                  Initiate Rekey: 0
Respond Rekey: 0
                  Child SA Rekey: 0
           Outgoing Init Request: 0                  Incoming
Init Request: 0
          Outgoing Init Response: 0                 Incoming
Init Response: 0
           Outgoing Auth Request: 0                  Incoming
Auth Request: 0
          Outgoing Auth Response: 0                 Incoming
Auth Response: 0
   Outgoing Create Child Request: 0          Incoming Create
Child Request: 0
  Outgoing Create Child Response: 0         Incoming Create
Child Response: 0
           Outgoing Info Request: 0                  Incoming
Info Request: 0
          Outgoing Info Response: 0                 Incoming
Info Response: 0
                Incoming Invalid: 0
Incoming Invalid SPI: 0
```

show vpn ipsec-group

Description View the VPN IPSec group information.

Syntax

```
show vpn ipsec-group {group-name}
```

Parameter	Description
group-name	Specify the IPsec group name. It can be 1-31 characters.
all-partitions	Shows IPsec group for all partitions. Without this option, group information is listed only for the partition from which you enter the command.

Default N/A

Mode All

Example The following command shows summary information for the IPsec group (group1) on the ACOS device.

```
ACOS#show vpn ipsec-group group1

Group_Name: group1
Name   IKE GW Name Status   Priority   Role
-------------------------------------------------------
a2     a2           UP       8          Primary
a1     a1           UP       7          Backup
```

Example The following command shows summary information for all the IPsec groups in the current partition.

```
ACOS#show vpn ipsec-group

Group_Name: group1
Name   IKE GW Name Status   Priority   Role
-------------------------------------------------------
a2     a2           UP       8          Primary
a1     a1           UP       7          Backup

Group_Name: group2
Name   IKE GW Name Status   Priority   Role
-------------------------------------------------------
a3                  DOWN       8         DOWN
a4                  DOWN       7         DOWN
a5                  DOWN       6         DOWN
```

The following table describes the fields in the above output:

Field	Description
Name	Name of the IPsec tunnel.
IKE GW Name	Name of the ike-gateway associated with the IPSec tunnel.
Status	Represents if the IPsec tunnel is established (UP) or not (DOWN).

Field	Description
Priority	Values configured at the time of group creation.
Role	Represents the role of the current group member. The role can be: • Primary - Indicates that the tunnel is used in passing traffic. The tunnel configured with the highest priority is designated as the Primary tunnel. • Backup - Indicates that the tunnel is UP however, the tunnel is not passing traffic. It can assume the role of the Primary tunnel, when the primary tunnel is down (for example, if the tunnel interface is disabled). • Disabled - Indicates that the tunnel interface is disabled. • DOWN - Indicates that the tunnels are not yet established.

show vpn ipsec-sa

Description Shows the IPsec SAs information.

- For the Multi-PU platforms, the `show vpn ipsec-sa <NAME>` output on PU1 displays aggregated information from PU1 and PU2.
- For the Multi-PU platforms, the `show vpn ipsec-sa <NAME>` output on PU2 displays information only from PU2.

Syntax

```
show vpn ipsec-sa {sa-name | all-partitions}
```

Parameter	Description
sa-name	Specify the IPsec SA name, 1-31 characters.
all-partitions	Show IPsec SA information for all partitions.

Default N/A

Mode All

Example

The following command shows summary information for the IKE SAs on the ACOS device. The name of the tunnel mentioned here is used to bring the tunnel UP or DOWN. The In/Out SPI is the index that identifies the tunnel in each direction. Anti-replay failure can be displayed using the *show vpn ipsec-sa p2 | include Anti-Replay Failure* command.

```
ACOS#show vpn ipsec-sa

Gateway:11    Local IP:70.70.70.1    Remote IP:70.70.70.2
Name  Selectors       In/Out SPI  Mode/xform   Time/Bytes
-----------------------------------------------------
11    50.50.50.0/24   0x5872a202  esp-tunnel   28787s
      51.51.51.0/24   0x0af8bfe9  aes-128-sha1 unlimited

ACOS#show vpn ipsec-sa [IPsec SA name]
SA Index: 1              Tunnel Name: 11
Local IP: 50.50.50.0/24
Peer IP: 51.51.51.0/24
Local SPI: 0x5872a202
Remote SPI: 0xaf8bfe9
Protocol: esp
Mode: tunnel
Encryption Algorithm: aes-128
Hash Algorithm: sha1
DH Group: 0
NAT-T: disabled
Anti-Replay: disabled
Encrypted Packets: 0
Encrypted Bytes: 0
Decrypted Packets: 0
Decrypted Bytes: 0
Bad SPI: 0
Rekey Times: 0
Pad Check Error: 0
ICV Check Error: 0
Anti-Replay Failure: 0
Sequence Number: 0
Sequence Number Rollover: 0
Lifetime: 28784
```

```
Lifebytes: unlimited
Pre-frag Success: 0
Frag-after-encap Fragment Generated: 0
Fragment Received: 0

#show vpn ipsec-sa ipv6
SA Index: 1          Tunnel Name: ipv6
Local IP: 3000:2000:c00:2::1/64
Peer IP: 2000:2000:c00:2::1/64
Local SPI: 0x1c41f226
Remote SPI: 0x27b42a8c
Protocol: esp                                          Mode:
tunnel
Encryption Algorithm: aes-256                            Hash
Algorithm: sha1
DH Group: 5
NAT-T: disabled
Anti-Replay: disabled
Encrypted Packets: 0                                  Encrypted
Bytes: 0
Decrypted Packets: 0                                  Decrypted
Bytes: 0
Anti-Replay Failure: 0                                      Rekey
Times: 31
Pad Check Error: 0
ICV Check Error: 0
Sequence Number: 0
Sequence Number Rollover: 0
Lifetime: 9911                                     Lifebytes:
unlimited
Pre-frag Success: 0
Pre-frag Error: 0
Frag-after-encap Fragment Generated: 0
Fragment Received: 0

ACOS#show vpn ipsec-sa all-partitions
Partition shared
Gateway:11    Local IP:70.70.70.1    Remote IP:70.70.70.2
Name  Selectors      In/Out SPI  Mode/xform   Time/Bytes
-------------------------------------------------------
```

```
11      50.50.50.0/24   0x5872a206   esp-tunnel     27903s
        51.51.51.0/24   0x0af8bfed   aes-128-sha1   unlimited
```

show vpn log

Description View the VPN log messages.

For the Multi-PU platforms, the `show vpn log` output is displayed only on PU1.

Syntax

```
show vpn log {follow | from-start | num-lines] | [begin | include | exclude | section}
```

Parameter	Description
`follow`	Displays recent log entries, and displays new entries as they are generated. **NOTE:** This option takes control of the CLI session and uses it exclusively for displaying the VPN log messages. To end this mode and re-access the command prompt, press Ctrl+C.
`from-start`	Lists the VPN log messages, starting with the first message in the buffer.
`num-lines num`	Displays the specified number of entries (lines), beginning with the newest (most recent) entry.

Default N/A

Mode All

show vpn ocsp

Description Show information for certificates that are being managed by the OCSP server.

Syntax

```
show vpn ocsp
```

Default N/A

Mode All

Example The following command shows OCSP information:

```
ACOS#show vpn ocsp
   subject:   "C=US, ST=MD, L=Baltimore, CN=Gateway2"
   issuer:    "DC=com, DC=a10lab, CN=AD03-CA"
   validity:  produced at Jan 09 02:54:50 UTC 2015
              usable till Jan 09 15:21:50 UTC 2015, ok
(expires in 11 hours)
  certificate status: GOOD
   subject:   "C=US, ST=MD, L=Baltimore, CN=Gateway2"
   issuer:    "DC=com, DC=a10lab, CN=AD03-CA"
   validity:  produced at Jan 09 03:09:03 UTC 2015
              usable till Jan 09 15:21:50 UTC 2015, ok
(expires in 11 hours)
  certificate status: UNKNOWN
Total: 2
```

Network Configuration

ACOS provides Layer 2, Layer 3, and Routing Protocols networking for configuring ACOS devices.

This reference lists the CLI configuration and show commands that apply specifically to network protocols.

Configuration Commands

interface

Description Access the CLI configuration level for an interface.

Syntax

```
interface {
ethernet port-num |
lif logical-interface-id |
loopback num |
management |
management2 |
trunk  num |
tunnel num |
ve ve-num
}
```

Parameter	Description
ethernet *port-num*	The configured interface is a virtual or physical Ethernet port with *port-num* ID. The port ID takes a range of values that depends of the platform ACOS is running on.
lif *logical-interface-id*	The configured interface is a logical interface in a Software Defined Network (SDN) or Overlay Network with *interface-id* ID. The logical interface ID takes a range of values from 1 to 128.

Parameter	Description
loopback *num*	The configured interface is a Layer 2 loopback interface.
management	The configured interface is a management interface of the ACOS Device. (For more information, see *System Configuration and Administration Guide*.)
management2	The configured interface is the second management interface of the ACOS Device. (For more information, see *System Configuration and Administration Guide*.) **NOTE:** The second management interface is available only for the Thunder 8665S platform.
trunk *num*	The configured interface is a logical trunk interface of the ACOS Device. The trunk interface ID associates the interface with a trunk group and takes a range of values from 1 to 4096.
tunnel *num*	The configured interface is a tunnel. The tunnel interface ID takes a range of values from 1 to 128. (For more information, see "Basic IPsec VPN Deployment" in the *Configuring IPsec VPN*.)
ve *ve-num*	The configured interface is a virtual Ethernet Interface. (For more information, see "Virtual LAN Support" in the *Network Configuration Guide*.) The virtual Ethernet ID takes a range of values that depends of the platform ACOS is running on.

Default N/A

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, specify the interface number as follows: *DeviceID*/*Portnum*

Example The following command changes the CLI to the configuration level for Ethernet interface 3:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)#
```

Example The following command changes the CLI to the configuration level for Interface management2:

```
ACOS(config)# interface management2
ACOS(config-if:management2)#
```

access-list

Description Apply an Access Control List (ACL) to an interface.

Prerequisite The ACL (access-list) must be configured before you can apply it to an interface.

Syntax

```
[no] access-list [num | name name] in
```

Parameter	Description
num	Number or ID of a configured ACL.
name	Name of a configured ACL.
in	Applies the ACL to inbound traffic received on the interface.

Default N/A

Mode Interface

Usage You can apply ACLs to Ethernet data interfaces, Virtual Ethernet (VE) interfaces, the management interface, trunks, and virtual server ports. Applying ACLs to the out-of-band management interface is not supported.

You can apply ACLs only to the inbound traffic direction. This restriction ensures that ACLs are used most efficiently by filtering traffic as it attempts to enter the ACOS device, before being further processed by the device.

Example The following commands configure a standard ACL to deny traffic from subnet 10.10.10.x, and apply the ACL to the inbound traffic direction on Ethernet interface 4:

```
ACOS(config)# access-list 1 deny 10.10.10.0 0.0.0.255
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# access-list 1 in
```

bfd

Description Enables or disables BFD on an individual interface.

Syntax

```
[no] bfd {authentication key-id {auth-type} | echo {demand} |
interval ms min-rx ms multiplier num | per-member-port{ipv4 |
ipv6}}
```

Parameter	Description
authentication *key-id* { **md5** | **meticulous-md5** | **meticulous-sha1** | **sha1** | **simple**}	The **authentication** option specifies the authentication type to be used for BFD. You can specify a key-id from 0-255. The authentication options include the following: • **md5** – Keyed MD5 • **meticulous-md5** – Meticulous keyed MD5 • **meticulous-sha1** –Meticulous keyedSHA1 • **sha1** – Keyed SHA1 • **simple** – Simple password **NOTE:** **The md5 and meticulous-md5 options are not supported in FIPS mode.**
echo [**demand**]	Specify **echo** mode. You can enable the **demand** mode to work in conjunction with the echo function. When demand mode is enabled (and a BFD session has been established), the system will be able to verify connectivity with another system at will instead of routinely.
interval *ms* **min-rx** *ms* **multiplier** *num*	The **interval** value is the transmit timer, and it specifies the rate at which the ACOS device sends BFD control packets to its BFD neighbors. You can specify 48-1000 milliseconds (ms). The default is 800 ms. This timer is used in Asynchronous mode only. The **min-rx** option is the detection timer, and this allows you to specify the maximum

Parameter	Description
	number of *ms* the ACOS device will wait for a BFD control packet from a BFD neighbor. The **min-rx** value can be 48-1000 ms, and is 800 ms by default. This timer is used in Asynchronous mode only. The **multiplier** value is the wait multiplier, and this enables you to specify the maximum number of consecutive times the ACOS device will wait for a BFD control packet from a neighbor. If the multiplier value is reached, the ACOS device concludes that the routing process on the neighbor is down. The **multiplier** value can be 3-50 and is 4 by default.
per-member-port [**ipv4** *{local-address | neighbor-address}* | **ipv6** *{local-address | neighbor-address}*]	Configures a Micro BFD. • **ipv4** - IPv4 BFD sessions. ◦ `local-address` - Specify the IPv4 local address. ◦ `neighbor-address` - Specify the IPv4 neighbor address. • **ipv6** - IPv6 BFD sessions. ◦ `local-address` - Specify the IPv6 local address. ◦ `neighbor-address` - Specify the IPv6 neighbor address.

Mode Interface

Usage If you configure the timers on an individual interface, the interface's settings are used instead of the global settings. Likewise, if the BFD timers are not set on an interface, that interface uses the global settings. For BGP loopback neighbors, BFD always uses the global timer.

NOTE: For a BFD session for BGP using a loopback address, for an OSPFv2 virtual link, and for an OSPFv3 virtual link, the ACOS device will always use the global timer regardless of the timer that is configured at the interface level.

Example The following example shows enabling BFD on an interface:

```
ACOS(config-if:ethernet:1)# bfd authentication 1 md5 password-string
```

The following example shows a BFD session for BGP:

```
ACOS(config)# router bgp 1
ACOS(config-bgp:1)# neighbor 1.2.3.4 fall-over bfd
authentication 1 md5 password-string
```

NOTE: The **fall-over bfd authentication md5** and **meticulous-md5** options are not supported in FIPS mode.

Example The following example shows a Micro-BFD session (IPv4) configuration for trunk member-port:

```
ACOS(config-if:trunk:2)# bfd per-member-port
ACOS(config-if:trunk:2-per-member-port)#ipv4 local-address
10.10.10.1
ACOS(config-if:trunk:2-per-member-port)#ipv4 neighbor-address
10.10.10.2
```

cpu-process

Description Enable software-based switching or routing of Layer 2/Layer 3 traffic.

NOTE: This command is only applicable on FTA-enabled devices.

Syntax

```
[no] cpu-process
```

Default Disabled. Traffic is switched or routed in hardware.

Mode Interface

dac-link-training-enable

Description Enables the Direct Attach Copper (DAC) cable link training to establish the link with the interface.

Syntax

```
[no] dac-link-training-enable
```

Mode Interface

Usage The DAC link training is the process that enables the DAC cable and a switch to negotiate the parameters and establish a reliable connection. This command is recommended only when the ACOS device is connected to the 400G DAC Copper cable and must interoperate with the Dell Fabric switch. It is not required for other switches.

Example The following command enables the DAC link training:

```
ACOS(config-if:ethernet:12)#dac-link-training-enable
```

disable

Description Disable an interface.

Syntax

```
disable
```

Default The management interface is enabled by default. Data interfaces are disabled by default.

Mode Interface

Usage This command applies to all interface types: Ethernet data interfaces, out-of-band Ethernet management interface, Virtual Ethernet (VE) interfaces, and loopback interfaces.

The command also applies to trunks. When you disable a trunk at the interface configuration level for the trunk, Layer 3 forwarding is disabled on the trunk.

In L3V deployments, tagged VLAN ports can be enabled or disabled only from the shared partition.

Example The following command disables Ethernet interface 3:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# disable
```

Example The following commands access the interface configuration level for trunk 7 and disable Layer 3 forwarding on the trunk:

```
ACOS(config)# interface trunk 7
ACOS(config-if:trunk:7)# disable
```

duplexity

Description Set the duplex mode for an Ethernet interface.

Syntax

```
[no] duplexity {Full | Half | auto}
```

Parameter	Description
Full	Full-duplex mode.
Half	Half-duplex mode.
auto	The mode is negotiated based on the mode of the other end of the link.

Default auto

Mode Interface

Usage This command applies only to physical interfaces (Ethernet ports or the management port).

Example The following command changes the mode on Ethernet interface 6 to half-duplex:

```
ACOS(config)# interface ethernet 6
ACOS(config-if:ethernet:6)# duplexity Half
```

enable

Description Enable an interface.

Syntax

```
enable
```

Default The management interface is enabled by default. Data interfaces are disabled by default.

Mode Interface

Usage This command applies to all interface types: Ethernet data interfaces, out-of-band Ethernet management interface, Virtual Ethernet (VE) interfaces, trunks, and loopback interfaces.

In L3V deployments, tagged VLAN ports can be enabled or disabled only from the shared partition.

Example The following command enables Ethernet interface 3:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# enable
```

flow-control

Description Enable 802.3x flow control on a full-duplex Ethernet interface.

Syntax

```
[no] flow-control
```

Default Disabled. The ACOS Ethernet interface auto-negotiates flow control settings with the other end of the link.

Mode Interface

Usage This command can cause the interface to briefly go down, then come back up again.

icmp-rate-limit

Description Configure ICMP rate limiting, to protect against denial-of-service (DoS) attacks.

Syntax

```
[no] icmp-rate-limit normal-rate [lockup max-rate lockup-time]
```

Parameter	Description
normal-rate	Maximum number of ICMP packets allowed per second on the interface. If the ACOS interface receives more than the normal rate of ICMP packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.

Parameter	Description
max-rate	Maximum number of ICMP packets allowed per second before the ACOS device locks up ICMP traffic on the interface. When ICMP traffic is locked up, all ICMP packets on the interface are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the ACOS device drops all ICMP traffic on the interface, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

Default None

Mode Global Config

Usage This command configures ICMP rate limiting on a physical, virtual Ethernet, trunk, or loopback interface. To configure it in a virtual server template, see slb template virtual-server. If you configure ICMP rate limiting filters at more than one of these levels, all filters are applicable.

Log messages are generated only if the **lockup** option is used and lockup occurs. Otherwise, the ICMP rate-limiting counters are still incremented but log messages are not generated.

Example The following command configures ICMP rate limiting on Ethernet interface 3:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# icmp-rate-limit 1024 lockup 1200
10
```

icmpv6-rate-limit

Description Configure ICMPv6 rate limiting, to protect against denial-of-service (DoS) attacks.

Syntax

```
[no] icmpv6-rate-limit normal-rate [lockup max-rate lockup-
time]
```

Parameter	Description
normal-rate	Maximum number of ICMPv6 packets allowed per second on the interface. If the ACOS interface receives more than the normal rate of ICMPv6 packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.
lockup *max-rate*	Maximum number of ICMPv6 packets allowed per second before the ACOS device locks up ICMPv6 traffic on the interface. When ICMPv6 traffic is locked up, all ICMPv6 packets on the interface are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the ACOS device drops all ICMPv6 traffic on the interface, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

Default None

Mode Global Config

Usage This command configures ICMPv6 rate limiting on a physical, virtual Ethernet, trunk, or loopback interface. To configure it in a virtual server template, see slb template virtual-server. If you configure ICMPv6 rate limiting filters at more than one of these levels, all filters are applicable.

Log messages are generated only if the **lockup** option is used and lockup occurs. Otherwise, the ICMPv6 rate-limiting counters are still incremented but log messages are not generated.

Example The following command configures ICMPv6 rate limiting on Ethernet interface 3:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# icmpv6-rate-limit 1024 lockup 1200
10
```

ip address

Description Assigns an IP address to an interface.

Syntax `[no] ip address ipaddr {subnet-mask | /mask-length}`

Default There are no IP addresses configured by default.

Mode Interface

Usage This command applies only when the ACOS device is used in gateway mode.

You can configure multiple IP addresses on Ethernet and Virtual Ethernet (VE) data interfaces, trunks, and on loopback interfaces, on ACOS devices deployed in gateway (route) mode.

NOTE: The IPv4 link-local address 169.254.x.x/16 is not supported.

Each IP address must be unique on the ACOS device. Addresses within a given subnet can be configured on only one interface on the device. (The ACOS device can have only one data interface in a given subnet.)

IP addresses are added to an interface in the order you configure them. The addresses appear in show command output and in the configuration in the same order.

The first IP address you add to an interface becomes the primary IP address for the interface. If you remove the primary address, the next address in the list (the second address to be added to the interface) becomes the primary address.

It does not matter which address is the primary address. OSPF can run on all subnets configured on a data interface.

The ACOS device automatically generates a directly connected route to each IP address. If you enable redistribution of directly connected routes, those protocols can advertise the routes to the IP addresses.

The ACOS device allows the same IP address to be configured as the ACOS device's global IP address, and as a NAT pool address. However, in Layer 2 (transparent) deployments, if you do configure the same

address in both places, and later delete one of the addresses, you must reload the ACOS device to place the change into effect.

Example The following command assigns IP address 10.2.4.69 to Ethernet interface 9:

```
ACOS(config-if:ethernet:9)# ip address 10.2.4.69 /24
```

Example The following commands configure multiple IP addresses on an Ethernet data interface, display the addresses, then delete the primary IP address and display the results.

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# ip address 10.10.10.1 /24
ACOS(config-if:ethernet:1)# ip address 10.10.20.2 /24
ACOS(config-if:ethernet:1)# ip address 20.20.20.1 /24
ACOS(config-if:ethernet:1)# show ip interfaces ethernet 1
  Ethernet 1 ip addresses:
  10.10.10.1 /24 (Primary)
  10.10.20.2 /24
  20.20.20.1 /24
ACOS(config-if:ethernet:1)#no ip address 10.10.20.2 /24
ACOS(config-if:ethernet:1)#show ip interfaces ethernet 1
  Ethernet 1 ip addresses:
  10.10.10.1 /24 (Primary)
  20.20.20.1 /24
```

ip address dhcp

Description Enable Dynamic Host Configuration Protocol (DHCP) to configure multiple IP addresses on an Ethernet data interface.

Syntax

```
[no] ip address dhcp
```

Default Disabled

Mode Interface

Usage You can configure VIPs and IP NAT pools to use the DHCP-assigned address of a given data interface. If this option is enabled, ACOS updates the VIP or pool address any time the specified data interface's IP address is changed by DHCP.

Additional Notes

- DHCP can be enabled on an interface only if that interface does not already have any statically assigned IP addresses.
- On ACOS devices deployed in gateway (Layer 3) mode, Ethernet data interfaces can have multiple IP addresses. An interface can have a combination of dynamically assigned addresses (by DHCP) and statically configured addresses. However, if you plan to use both methods of address configuration, static addresses can be configured only after you finish using DHCP to dynamically configure addresses. To use DHCP in this case, you must first delete all the statically configured IP addresses from the interface.
- On virtual appliance models, if single-IP mode is used, DHCP can be enabled only at the physical interface level.
- On devices deployed in Transparent (Layer 2) mode:
  - you can enable DHCP on the management interface and at the global level.
  - The VIP address and pool NAT address (if used) should match the global data IP address of the device. Make sure to enable this option when configuring the VIP or pool.

ip allow-promiscuous-vip

Description Enable client traffic received on this interface and addressed to TCP port 80 to be load balanced for any VIP address.

Syntax

```
[no] ip allow-promiscuous-vip
```

Default Disabled

Mode Interface

Usage This feature also requires configuration of a virtual server that has IP address 0.0.0.0. For more information, refer *Application Delivery and Server Load Balancing Guide*.

ip cache-spoofing-port

Description Configure the interface to support a spoofing cache server. A spoofing cache server uses the client's IP address instead of its own as the

source address when obtaining content requested by the client.

Syntax `[no] ip cache-spoofing-port`

Default Disabled

Mode Interface

Usage This command applies to the Transparent Cache Switching (TCS) feature. Enter the command on the interface that is attached to the spoofing cache. For more information, see *Application Delivery Controller Guide*.

Example The following command configures interface 9 to support a spoofing cache server that is attached to the interface.

```
ACOS(config-if:ethernet:9)# ip cache-spoofing-port
```

ip client

Description Enable client facing interface for IPv4 or IPv6 traffic.

Syntax `[no] ip client`

Default Not enabled

Mode Interface

Usage This command will look for the client's source IP for hashing. It is useful for hash-based load balancing.

Example The following command configure the interfaces on the client-side for IPv6:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# ip address 10.1.1.47 255.255.255.0
ACOS(config-if:ethernet:1)# ip client
ACOS(config-if:ethernet:1)# ipv6 address 1000::47/64
ACOS(config-if:ethernet:)# exit
```

Related Commands:

- ip server
- system same-src-port-ip-hash

ip control-apps-use-mgmt-port

Description Enables use of the management interface as the source interface for automated management traffic.

NOTE: This command is valid for the management interface only.

Limitation When the VCS floating IP is configured and the **`ip control-apps-use-mgmt-port`** setting is applied on the device, the SSHd service is updated to reflect this. As a result, if the SSH connection is restarted, the VCS floating IP will fail to respond.

Syntax

```
[no] ip control-apps-use-mgmt-port
```

Default By default, use of the management interface as the source interface for automated management traffic is disabled.

Mode Interface

Usage The ACOS device uses separate route tables for management traffic and data traffic.

- Management route table – Contains all static routes whose next hops are connected to the management interface. The management route table also contains the route to the device configured as the management default gateway.
- Main route table – Contains all routes whose next hop are connected to a data interface. Also contains copies of all static routes in the management route table, excluding the management default gateway route. Only the data routes are used for load-balanced traffic.

By default, the ACOS device attempts to use a route from the main route table for management connections originated on the ACOS device. The **`ip control-apps-use-mgmt-port`** command enables the ACOS device to use the management route table for these connections instead.

The ACOS device uses the management route table to send reply traffic for connections initiated by a remote host that reaches the ACOS device on the management port. For example, this occurs for SSH or HTTP connections from remote hosts to the ACOS device.

Example The following command enables use of the management interface as the source interface for automated management traffic:

```
ACOS(config-if:management)# ip control-apps-use-mgmt-port
```

ip default-gateway

Description Specify the default gateway for the out-of-band management interface.

NOTE: This command is valid for the management interface only.

Syntax

```
[no] ip default-gateway ipaddr
```

Default None

Mode Interface

Usage Configuring a default gateway for the management interface provides the following benefits:

- Ensures that reply management traffic sent by the ACOS device travels through the correct gateway
- Keeps reply management traffic off the data interfaces

The default gateway configured on the management interface applies only to traffic sent from this interface. For traffic sent through data interfaces, either the globally configured default gateway is used instead (if the ACOS device is deployed in transparent mode) or an IP route is used (if the ACOS device is deployed in route mode).

To configure the default gateway for data interfaces on an ACOS device deployed in transparent mode, use the **ip default-gateway** command at the Global configuration level. (See “ip default-gateway” in the *Command Line Interface Reference*.)

NOTE: Normally, if the ACOS device is deployed in transparent mode, outbound traffic through the management interface is limited to the same subnet. However, outbound traffic through data interfaces is not restricted to the same subnet. To perform operations that require exchanging files with a host (upgrade, import, export, and so on) that is in a different subnet from the management interface:

- Use the **ip control-apps-use-mgmt-port** command to configure automated management traffic such as syslog messages and SNMP traps.
- For management traffic that you initiate using a command, use the **use-mgmt-port** option with the command.

Example The following commands configure an IP address and default gateway for the management interface:

```
ACOS(config)# interface management
ACOS(config-if:management)# ip address 10.10.20.1 /24
ACOS(config-if:management)# ip default-gateway 10.10.20.1
```

ip helper-address

Description Configure a helper address for Dynamic Host Configuration Protocol (DHCP).

Syntax

```
[no] ip helper-address ipaddr
```

Replace *ipaddr* with the IP address of the DHCP server.

Default None

Mode Interface

Usage In the current release, the helper-address feature provides service for DHCP packets only.

The ACOS interface on which the helper address is configured must have an IP address.

The helper address cannot be the same as the IP address on any ACOS interface or an IP address used for SLB.

The current release supports DHCP relay service for IPv4 only.

Example The following commands configure two helper addresses. The helper address for DHCP server 100.100.100.1 is configured on ACOS Ethernet interface 1 and on Virtual Ethernet (VE) interfaces 5 and 7. The helper address for DHCP server 20.20.20.102 is configured on VE 9.

```
ACOS(config)# interface ethernet 1
```

```
ACOS(config-if:ethernet:1)# ip helper-address 100.100.100.1
ACOS(config-if:ethernet:1)# exit
ACOS(config)# interface ve 5
ACOS(config-if:ve:5)# ip helper-address 100.100.100.1
ACOS(config-if:ve:5)# exit
ACOS(config)# interface ve 7
ACOS(config-if:ve:7)# ip helper-address 100.100.100.1
ACOS(config-if:ve:7)# exit
ACOS(config)# interface ve 9
ACOS(config-if:ve9)# ip helper-address 20.20.20.102
```

ip igmp

Description Configure IGMPv2 membership request queries.

Syntax

```
[no] ip igmp generate-membership-query query-timer  max-resp-time response-timer
```

Parameter	Description
query-timer	Sets the time interval (1-255 seconds) after which your device (using the interface under which you are configuring this feature) will initiate an IGMP membership query request. The default query timer is 125 seconds. This means that IGMP membership queries will be sent every 125 seconds from the configured interface.
response-timer	Sets the time interval (in 1/10 of a second) before which receiving devices will send an ICMP query message response to indicate intention to join the IGMP group or not. The default response timer is 100. This means that receiving devices have 10 seconds in which to indicate if they will join the IGMP membership group or not.

Default None

Mode Interface

Usage The configured timer is valid only per interface and it must be set for each individual interface.

Example To configure IGMP membership request queries on a physical interface, do the following:

```
ACOS(config-if)# interface ethernet 2
ACOS(config-if:ethernet:2)# ip address 192.168.1.1 /24
ACOS(config-if:ethernet:2)# ip igmp generate-membership-query
10 max-resp-time 50
```

To view your IGMP membership request query configuration for a a physical interface, do the following:

```
ACOS(config)# show interfaces ethernet 2
  Ethernet 2 is up, line protocol is up
  Hardware is GigabitEthernet, Address is 001f.a004.2e71
  Internet address is 192.168.1.1, Subnet mask is
255.255.255.0
  Configured Speed auto, Actual 1Gbit, Configured Duplex auto,
Actual fdx
  IGMP Membership Query is enabled, IGMP Membership Queries
sent 3
  Flow Control is disabled, IP MTU is 1500 bytes
  Port as Mirror disabled, Monitoring this Port disabled
  0 packets input,  0 bytes
  Received 0 broadcasts,  Received 0 multicasts,  Received 0
unicasts
  0 input errors,  0 CRC  0 frame
  0 runts  0 giants
  3003 packets output  264264 bytes
  Transmitted 0 broadcasts  3003 multicasts  0 unicasts
  0 output errors  0 collisions
  300 second input rate: 0 bits/sec, 0 packets/sec, 0%
utilization
  300 second output rate: 12768 bits/sec, 18 packets/sec, 0%
utilization
```

Example To configure IGMP membership request queries on an virtual Ethernet interface, do the following:

```
ACOS(config)# vlan 50
ACOS(config-vlan:50)# tagged ethernet 1
ACOS(config-vlan:50)# router-interface ve 50
ACOS(config-vlan:50)# exit
```

```
ACOS(config)# interface ve 50
ACOS(config-if:ve:50)# ip address 10.10.10.219 /24
ACOS(config-if:ve:50)#  ip igmp generate-membership-query 10
max-resp-time 50
```

To view your IGMP membership request query configuration for a virtual Ethernet interface, do the following:

```
ACOS(config)# show interfaces ve 50
VirtualEthernet 50 is up, line protocol is up
  Hardware is VirtualEthernet, Address is 001f.a004.2e72
  Internet address is 10.10.10.219, Subnet mask is
255.255.255.0
  Router Interface for L2 Vlan 50
  IP MTU is 1500 bytes
  IGMP Membership Query is enabled, IGMP Membership Queries
sent 32
  0 packets input  0 bytes
  Received  0 broadcasts, Received 0 multicasts, Received 0
unicasts
  0 packets output  0 bytes
  Transmitted  0 broadcasts, Transmitted 0 multicasts,
Transmitted 0 unicasts
  300 second input rate: 0 bits/sec, 0 packets/sec
  300 second output rate: 0 bits/sec, 0 packets/sec
```

Example

To configure IGMP membership request queries on a trunk, do the following:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# trunk-group 3
ACOS(config-if:ethernet:3-trunk-group:3)# exit
ACOS(config-if:ethernet:3)# exit
ACOS(config)# interface trunk 3
ACOS(config-if:trunk:3)# enable
ACOS(config-if:trunk:3)# ip address 11.11.11.219 /24
ACOS(config-if:trunk:3)# ip igmp generate-membership-query 20
max-resp-time 80
ACOS(config-if:trunk:3)# exit
```

To view your IGMP membership request query configuration for a trunk, do the following:

```
ACOS(config)# show interfaces trunk 3
Trunk 3 is up, line protocol is up
  Hardware is TrunkGroup, Address is 001f.a011.1a4f
  Internet address is 11.11.11.219, Subnet mask is
255.255.255.0
  IP MTU is 1500 bytes
  IGMP Membership Query is enabled, IGMP Membership Queries
sent 0
```

ip nat

Description Enable source Network Address Translation (NAT) on an interface.

Syntax

```
[no] ip nat {inside | outside}
```

Parameter	Description
inside	Specifies that this interface is connected to the internal hosts on the private network that need to be translated into external addresses for routing.
outside	Specifies that this interface is connected to the external network or Internet. Before sending traffic from an inside host out on this interface, the ACOS device translates the host's private address into a public, routable address.

Default None

Mode Interface

Usage On an ACOS device deployed in transparent mode, this command is valid only on Ethernet data ports. On an ACOS device deployed in route mode, this command is valid on Ethernet data ports, Virtual Ethernet (VE) interfaces, and trunks.

To use source NAT, you also must configure global NAT parameters.

In addition, on some AX series models, if Layer 2 IP NAT is required, you also must enable cpu-process on the interface. This applies to AX models AX 3200-12, AX 3400, AX 5200-11, and AX 5630.

Example

The following commands configure IP source NAT for internal addresses in the 10.1.1.x/24 subnet connected to interface 14. The addresses are translated into addresses in the range 10.153.60.120-150 before traffic from the internal hosts is sent onto the Internet on interface 15. Likewise, return traffic is translated back from public addresses into the private host addresses.

```
ACOS(config)# access-list 3 permit 10.1.1.0 0.0.0.255
ACOS(config)# ip nat pool 1 10.153.60.120 10.153.60.150
netmask /24
ACOS(config)# ip nat inside source list 3 pool 1
ACOS(config)# interface ethernet 14
ACOS(config-if:ethernet:14)# ip address 10.1.1.1
255.255.255.0
ACOS(config-if:ethernet:14)# ip nat inside
ACOS(config-if:ethernet:14)# exit
ACOS(config)# interface ethernet 15
ACOS(config-if:ethernet:15)# ip address 10.153.60.100
255.255.255.0
ACOS(config-if:ethernet:15)# ip nat outside
```

ip ospf

Description

Configures OSPF interface settings.

Syntax

```
[no] ip ospf {
[ipaddr] authentication [message-digest | null] |
[ipaddr] authentication-key key-string |
bfd [disable] |
[ipaddr] cost number |
[ipaddr] database-filter all out |
[ipaddr] dead-interval seconds |
disable all |
[ipaddr] hello-interval seconds |
[ipaddr] message-digest-key key-id md5 key-string |
mtu size |
[ipaddr] mtu-ignore |
network type |
[ipaddr] priority priority |
[ipaddr] retransmit-interval seconds |
[ipaddr] transmit-delay seconds
}
```

Parameter	Description
ipaddr	Configures the parameter only for the specified IP address. Without this option, the parameter is configured for all IP addresses on the interface.
authentication	ype of authentication used to validate OSPF route updates sent or received on this interface: • **message-digest** – Message Digest 5 (MD5) • **null** – No authentication is used. If you enter the authentication command without either of the options above, a simple key is used for authentication. **NOTE:** The **message-digest** option is not supported in FIPS mode.
authentication-key *key-string*	Password used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. Applies to simple authentication only. Can be a string up to 8 characters long, with no blanks.
bfd	Sets BFD on the interface. BFD on the interface is disabled by default.
cost *number*	Numeric cost for using the interface, 1-65535. By default, an interface's cost is calculated based on the interface's bandwidth. If the auto-cost reference bandwidth is set to its default value (100 Mbps), the default interface cost is 10.
database-filter all out	Blocks flooding of LSAs to the OSPF interface. This is disabled by default; LSA flooding is

Parameter	Description
	permitted
dead-interval *seconds*	Number of seconds that neighbor OSPF routers will wait for a new OSPF Hello packet from ACOS before declaring this OSPF router (the ACOS device) to be down, 1-65535 seconds. The default is 40 seconds.
disable all	Disables all OSPF packet processing on the interface.
hello-interval *seconds*	Number of seconds between transmission of OSPF Hello packets on this interface, 1-65535 seconds. The default is 10 seconds.
message-digest-key *key-id* **md5** *key-string*	Set of MD passwords used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. You can enter up to four key strings. Applies only to MD authentication. Key strings can be up to 16 characters long, with no blanks. **NOTE:** The **message-digest-key** option is not supported in FIPS mode.
mtu	Specifies the Maximum Transmission Unit (MTU) for OSPF packets transmitted on the interface. You can specify 576-65535 bytes. By default, the IP MTU set on the interface is used.
mtu-ignore	Disables MTU size checking during Database Description (DD) exchange. This option is useful when the MTU at the remote end of the link is larger than the maximum MTU supported on the local end of the link.

Parameter	Description
	By default, MTU size checking is enabled. If the MTU size in DD packets from a neighbor does not match the interface MTU, adjacency is not established
network *type*	OSPF network type from the default for the media. You can specify one of the following: • **broadcast** – Broadcast network. • **non-broadcast** – Non-broadcast multiaccess (NBMA) network. • **point-to-multipoint** – Point-to-multipoint network. • **point-to-point** – Point-to-point network. The default network type depends on the media type.
priority *number*	Eligibility of this OSPF router to be elected as the designated router (DR) or backup designated router (BDRs) for the routing domain, 0-255. 1 is the lowest priority and 255 is the highest priority. The default priority is 1.
retransmit-interval *seconds*	Number of seconds between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface, 1-65535 seconds. The default is 5 seconds.
transmit-delay *seconds*	Number of seconds it takes to transmit Link State Update packets (route updates) on this interface, 1-65535 seconds. This amount is added to the ages of LSAs sent in the updates. The default is 1 second.

Mode Interface

Usage The OSPF router with the highest priority is elected as the DR and the router with the second highest priority is elected as the BDR. If more than one router has the highest priority, the router with the highest OSPF router ID is selected. Priority applies only to multi-access networks, not to point-to-point networks. If you set the priority to 0, the Thunder Series does not participate in DR and BDR election.

Example The following command sets the OSPF priority on Ethernet interface 10 to 100:

```
ACOS(config)# interface ethernet 10
ACOS(config-if:ethernet:10)# ip ospf priority 100
```

ip rip authentication

Description Configure IPv4 RIP authentication on the interface.

Syntax

```
[no] ip rip authentication
{
  key-chain name [name ...] |
  mode {md5 | text} |
  string auth-string [auth-string ...]
}
```

Parameter	Description
key-chain *name* [*name* ...]	Enables authentication using the specified key chains. (To configure a key-chain file, use the **key chain** command at the global configuration level of the CLI.)
mode {**md5** | **text**}	Authentication mode: • **md5** – Message Digest 5 • **text** – Clear text **NOTE:** The **md5** option is not supported in FIPS mode.
string *auth-string* [*auth-string* ...]	Enables authentication using the specified passwords.

Default None

Mode Interface

ip rip receive version

Description Specify the RIP version allowed in RIP packets received on the interface.

Syntax

```
[no] ip rip receive version {1 [2] | 2}
```

Specify the RIP version:

- 1 - RIP version 1.
- 2 - RIP version 2 (default).

Default See descriptions.

Mode Interface

ip rip receive-packet

Description Enable the interface to receive RIP packets.

Syntax

```
[no] ip rip receive-packet
```

Default Enabled

Mode Interface

ip rip send version

Description Specify the RIP version allowed to be sent on the interface.

Syntax

```
[no] ip rip send version {1 [2] | 2}
```

Specify the RIP version:

- 1 - RIP version 1.
- 2 - RIP version 2 (default).

Default See descriptions.

Mode Interface

ip rip send-packet

Description Enable the interface to send RIP packets.

Syntax

```
[no] ip rip send-packet
```

Default Enabled

Mode Interface

ip rip split-horizon

Description Configure the split-horizon method. Split horizon prevents the ACOS device from advertising a route to the neighbor that advertised the same route to the ACOS device.

Syntax

```
[no] ip rip split-horizon {poisoned | disable | enable}
```

Parameter	Description
poisoned	Enables advertisement of a route to the neighbor that advertised the route to the ACOS device, but sets the metric value to infinity, thus making the route advertised by the ACOS device unusable by the neighbor (poisoned reverse). Without this option, advertisement of a route to the neighbor that advertised the route to the ACOS device is not allowed.
disable	Disable the split-horizon method.
enable	Enables split-horizon, but without the poisoned reverse.

Default Split-horizon with poison is enabled.

Mode Interface

ip router isis | ipv6 router isis

Description Enable Intermediate System to Intermediate System (IS-IS) routing on the interface.

Syntax

```
[no] {ip | ipv6} router isis [tag]
```

Default Not set

Mode Interface

ip server

Description Enable server facing interface for IPv4 or IPv6 traffic.

Syntax

```
[no] ip server
```

Default Not enabled.

Mode Interface

Usage This command will look for the destination IP (which is that of the client) for hashing and matching the session.

Example The following command configure the interfaces on the server-side for IPv6:

```
ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# ip address 30.1.1.47 255.255.255.0
ACOS(config-if:ethernet:2)# ip server
ACOS(config-if:ethernet:2)# ipv6 address 3000::47/64
ACOS(config-if:ethernet:2)# exit
```

Related Commands:

- ip client
- system same-src-port-ip-hash

ip slb-partition-redirect

Description Enable routing redirection on an ingress Ethernet data port that will receive traffic addressed to the VIP in a private partition.

Syntax

```
[no] ip slb-partition-redirect
```

Default Not set

Mode Interface

Example The following example enables routing redirection on ethernet interface 4 so that traffic addressed to partition p69 will be received on the partition.

```
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# ip slb-partition-redirect
ACOS(config-if:ethernet:4)# exit
ACOS(config)# ip route 10.2.4.0 /24 partition p69
ACOS(config)# active-partition p69
ACOS(config)# ip route 0.0.0.0 /24 partition shared
```

ip stateful-firewall

Description Configure stateful firewall direction for this interface.

Syntax

```
[no] ipv6 stateful-firewall {inside | outside [access-list num]}
```

Parameter	Description
inside	Inside (private) interface for the stateful firewall.
outside	Outside (public) interface for the stateful firewall.
access-list	Access list id. You can specify 1-199.

Mode Interface

Example The following configures stateful firewall on Ethernet interface 1.

```
ACOS(config-if:ethernet:1)# ip stateful-firewall outside
access-list 1
```

ip ttl-ignore

Description Configures the device to not decrement TTL field contents for IPv4 traffic passing through. By default TTL decrements for traffic passing through the ACOS device.

Syntax

```
[no] ip ttl-ignore
```

Default Not set

Mode Interface

Example The following example programs the device to not decrement TTL field contents for traffic passing through the ACOS device.

```
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# ip ttl-ignore
ACOS(config-if:ethernet:4)# exit
```

ipv6 (on management interface)

Description Configure an IP version 6 address and default gateway on the management interface.

Syntax

```
[no] ipv6 default-gateway gateway-ipaddr
[no] ipv6 addressipaddr/mask-length
```

Default None.

Mode Interface

Usage The **ipv6 default-gateway** command applies only to the management interface.

Example The following commands configure an IPv6 address and default gateway on the management port:

```
ACOS(config-if:management)# ipv6 address 2001:db8:11:2/32
ACOS(config-if:management)# ipv6 default-gateway
2001:db8:11:1/32
```

Related Commands:

- ipv6 address

ipv6 access-list

Description Apply an IPv6 Access Control List (ACL) to an interface.

Syntax

```
[no] ipv6 access-list name in
```

Parameter	Description
name	Name of a configured IPv6 ACL.
in	Applies the ACL to inbound IPv6 traffic received on the interface.

Default N/A

Mode Interface

ipv6 address

Description Configures an IPv6 address on the interface.

Syntax

```
[no]  ipv6 address ipv6-addr/prefix-length [link-local]
[anycast]
```

Parameter	Description
ipv6-addr	Valid unicast IPv6 address.
prefix-length	Prefix length, up to 128.
link-local	Configures the address as the link-local IPv6 address for the interface, instead of a global address. Without this option, the address is a global address.
anycast	Configures the address as an anycast address. An anycast address can be assigned to more than one interface. A packet sent to an anycast address is routed to the "nearest" interface with that address, based on the distance in the routing protocol.

Default None.

Mode Interface

Usage Use this command to configure the link-local and global IP addresses for the interface.

- The **ipv6 address** command, used without the **link-local** option, configures a global address. If you use the **link-local** option, the address is instead configured as the link-local address.
- To enable automatic configuration of the link-local IPv6 address instead, use the **ipv6 enable** command.

Example The following command configures a global IPv6 address on Ethernet interface 8:

```
ACOS(config-if:ethernet:8)# ipv6 address e101::1112/64
```

Example The following command overrides any auto-generated link-local address on interface 6 and explicitly configures a new link-local address:

```
ACOS(config-if:ethernet:6)# ipv6 address fe80::1/64 link-local
```

Related Commands:

- ipv6 (on management interface)

ipv6 enable

Description Enable automatic configuration of a link-local IPv6 address on the interface.

Syntax

```
[no] ipv6 enable
```

Default Disabled

Mode Interface

Usage Use this command to enable automatic configuration of the link-local IPv6 address.

Example The following command enables an automatically generated link-local IPv6 address on Ethernet interface 6:

```
ACOS(config)# interface ethernet 6
ACOS(config-if:ethernet:6)# ipv6 enable
```

Related Commands:

- ipv6 address

ipv6 nat inside

Description Enable inside NAT on the interface.

Syntax

```
[no] ipv6 nat inside
```

Default Disabled

Mode Interface

ipv6 nat outside

Description Enable outside NAT for IPv6 on the interface.

Syntax `[no] ipv6 nat outside`

Default Disabled

Mode Interface

ipv6 ndisc router-advertisement

Description Configure IPv6 neighbor router discovery (RFC 4861).

Syntax

```
[no] ipv6 ndisc router-advertisement
{ default-lifetime seconds |
disable |
enable |
hop-limit num |
managed-configuration-flag {enable | disable}|
max-interval seconds |
min-interval seconds |
mtu {disable | bytes} |
other-configuration-flag {enable | disable} |
prefix ipv6-addr/prefix-length
   [not-autonomous | not-on-link |
   preferred-lifetime seconds |
   valid-lifetime seconds] |
rate-limit num |
reachable-time ms |
retransmit-timer seconds |
vrid num}
```

Parameter	Description
default-lifetime *seconds*	Specifies the number of seconds for which router advertisements sent on this interface are valid. You can specify 0 or 4-9000 seconds. The value cannot be less than the maximum advertisement interval. If you specify 0, the host will not use this interface (IPv6 router) as a default route. The default lifetime is 1800 seconds.
disable	Disables IPv6 router discovery (default).
enable	Enables IPv6 router discovery (by default, this is disabled).
hop-limit *num*	Specifies the default hop count value that should be used by hosts. For a given packet, the

Parameter	Description
	hop count is decremented at each router hop. If the hop count reaches 0, the packet becomes invalid. You can specify 0-255. If you specify 0, the value is unspecified by this IPv6 router. The default is 255.
managed-configuration-flag {**enable** | **disable**}	Set the 1-bit "managed address configuration" flag, which enables addresses to be available via DHCP. For more information, see RFC 4861.
max-interval *seconds*	Specifies the maximum number of seconds between transmission of unsolicited router advertisement messages on this interface. You can specify 4-1800 seconds. The default is 600 seconds.
min-interval *seconds*	Specifies the minimum number of seconds between transmission of unsolicited router advertisement messages on this interface. You can specify 3-1350 seconds. The default is 200 seconds.
mtu {**disable** | **bytes**}	Specifies the MTU value to include in the MTU options field. You can specify 1200-9216 bytes or **disabled**. **NOTE:** If this option is disabled, no MTU value is included. This is disabled by default.
other-configuration-flag { **enable** |	Set the 1-bit "other address configuration" flag, which indicates that "other" information is available via DHCP.

Parameter	Description
disable }	For more information, seeRFC 4861.
prefix *ipv6-addr/prefix-length* [*options*]	Specifies the IPv6 prefixes to advertise on this interface. A maximum of 32 prefixes can be advertised on an interface. The following options are supported: • **not-autonomous** – Disables support for auto-configuration of IPv6 addresses by clients. This is disabled by default. • **not-on-link** – Disables the On-Link flag. When enabled, the On-Link flag indicates that the prefix is assigned to this interface. If you enable this option, the **valid-lifetime** is 2592000 seconds (30 days). This is enabled by default. • **preferred-lifetime** *seconds* – Specifies the number of seconds for which auto-generated addresses remain preferred. You can specify 0-4294967295 seconds. The default is 604800. • **valid-lifetime** *seconds* – specifies the number of seconds for which advertisement of the prefix is valid. You can specify 1-4294967295 seconds. The default is 2592000.
rate-limit *num*	Specifies the maximum number of router solicitation requests per second that will be processed on the interface. You can specify 1-100000 messages per second. The default rate limit is 00000 messages per second
reachable-time	Specifies the number of milliseconds (ms) for

Parameter	Description
ms	which the host should assume a neighbor is reachable, after receiving a reachability confirmation from the neighbor. You can specify 0-3600000 ms. If you specify 0, the value is unspecified by this IPv6 router. The default is 0.
retransmit-timer *seconds*	Specifies the number of seconds a host should wait between sending neighbor solicitation messages. You can specify 0-4294967295 seconds. If you specify 0, the value is unspecified by this IPv6 router. The default is 0.
vrid *num*	Specifies a VRID for which to send router advertisements. By default, no VRID is set; advertisement are sent regardless of VRID.

Default IPv6 router discovery is disabled by default. The command options have the default values specified in the table above.

Mode Interface

Usage When router discovery is enabled, the ACOS device:

- Sends IPv6 router advertisements out the IPv6 interfaces on which router discovery is enabled. IPv6 hosts that receive the router advertisements will use the ACOS device as their default gateway.
- Replies to IPv6 router solicitations received by IPv6 interfaces on which router discovery is enabled.

IPv6 router discovery is not supported in transparent mode. The ACOS device must be deployed in gateway mode.

When IPv6 router discovery is enabled on an interface, any new IPv6 addresses that you add to the interface are automatically added to the set of prefixes to advertise.

Router advertisements are sent to the all-nodes multicast address at an interval that is uniformly distributed between the minimum and maximum advertisement intervals. If a host sends a router solicitation message, the ACOS device sends a router advertisement as a unicast to that host instead.

The source address of router advertisements is always a link-local IPv6 address.

For the **reachable-time**, **hop-limit**, and **retransmit-timer** options, the ACOS device recommends the configured value to hosts but does not itself use the value.

Example The following commands configure an IPv6 address on Ethernet interface 1, enable IPv6 router discovery, change the minimum and maximum advertisement intervals, and add two prefixes to the prefix advertisement list.

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# ipv6 address 2001::1/64
ACOS(config-if:ethernet:1)# ipv6 ndisc router-advertisement
enable
ACOS(config-if:ethernet:1)# ipv6 ndisc router-advertisement
max-interval 300
ACOS(config-if:ethernet:1)# ipv6 ndisc router-advertisement
min-interval 150
ACOS(config-if:ethernet:1)# ipv6 ndisc router-advertisement
prefix 2001::/64 on-link
ACOS(config-if:ethernet:1)# ipv6 ndisc router-advertisement
prefix 2001:a::/96 on-link
```

ipv6 ospf cost

Description Explicitly set the link-state metric (cost) for this OSPF interface.

Syntax

```
[no] ipv6 ospf cost num
```

Replace *num* with the cost (1-65535).

Default By default, an interface's cost is calculated based on the interface's bandwidth. If the auto-cost reference bandwidth is set to its default value (100 Mbps), the default interface cost is 10.

Mode Interface

ipv6 ospf dead-interval

Description Specify the maximum time to wait for a reply to a hello message, before declaring the neighbor to be offline.

Syntax

```
[no] ipv6 ospf dead-interval seconds
```

Replace *seconds* with the number of seconds this OSPF router will wait for a reply to a hello message sent out this interface to an OSPF neighbor, before declaring the neighbor to be offline. You can specify 1-65535 seconds.

Default 40

Mode Interface

ipv6 ospf hello-interval

Description Specify the time to wait between sending hello packets to OSPF neighbors.

Syntax

```
[no] ipv6 ospf hello-interval seconds
```

Replace *seconds* with the number of seconds this OSPF router will wait between transmission of hello packets out this interface to OSPF neighbors. You can specify 1-65535 seconds.

Default 10

Mode Interface

ipv6 ospf mtu-ignore

Description Disable checking of the maximum transmission unit (MTU) during OSPFv3 Database Description (DD) exchange.

Syntax

```
[no] ipv6 ospf mtu-ignore [instance-id num ]
```

Replace *num* with a specific an OSPFv3 process, 0-255. If you do not use this option, MTU checking on the interface is disabled for all OSPFv3 processes.

Default MTU checking is enabled by default.

Mode Interface

ipv6 ospf neighbor

Description Configure an OSPFv3 neighbor that is located on a non-broadcast network reachable through this interface.

Syntax

```
[no] ipv6 ospf neighbor ipv6-addr
[
cost num [instance-id num] |
instance-id num |
poll-interval seconds [priority num] [instance-id num] |
priority num [poll-interval seconds] [instance-id num]
]
```

Parameter	Description
ipv6-addr	IPv6 address of the OSPF neighbor.
cost *num*	Specifies the link-state metric to the neighbor, 1-65535. There is no default cost set.
poll-interval *seconds*	Number of seconds this OSPFv3 interface will wait for a reply to a hello message sent to the neighbor, before declaring the neighbor to be offline. You can specify 1-4294967295 seconds. The default is 120 seconds.
priority *num*	Router priority of the neighbor, 1-255. The default priority is 0.

Default No neighbors on non-broadcast networks are configured by default. When you configure one, the other parameters have the default settings described in the table above.

ipv6 ospf network

Description Specify the network type.

Syntax

```
[no] ipv6 ospf network
{broadcast | non-broadcast | point-to-multipoint | point-to-
point}
[instance-id num]
```

Parameter	Description
broadcast	Broadcast network.
non-broadcast	Non-broadcast multiaccess (NBMA) network.
point-to-multipoint	Point-to-multipoint network.
point-to-point	Point-to-point network.
num	Specifies an OSPFv3 process, 0-255. If you do not use this option, MTU checking on the interface is disabled for all OSPFv3 processes.

Default Depends on the media type.

Mode Interface

ipv6 ospf priority

Description Priority of this OSPF router (and process) on this interface for becoming the designated router for the OSPF domain.

Syntax

```
[no] ipv6 ospf priority num
```

Replace *num* with the priority of this OSPF process on this interface, 0-255. The lowest priority is 0 and the highest priority is 255.

Default 1

Mode Interface

Usage If more than one OSPF router has the highest priority, the router with the highest router ID is selected as the designated router.

ipv6 ospf retransmit-interval

Description Specify the time to wait before resending an unacknowledged packet out this interface to an OSPF neighbor.

Syntax `[no] ipv6 ospf retransmit-interval seconds`

Replace *seconds* with the number of seconds this OSPF router waits before resending an unacknowledged packet out this interface to a neighbor. You can specify 1-65535 seconds.

Default 5

Mode Interface

ipv6 ospf transmit-delay

Description Specify the time to wait between sending packets out this interface to an OSPF neighbor.

Syntax `[no] ipv6 ospf transmit-delay seconds`

Replace *seconds* with the number of seconds this OSPF router waits between transmission of packets out this interface to OSPF neighbors. You can specify 1-65535 seconds.

Default 1

Mode Interface

ipv6 rip split-horizon

Description Configure the split-horizon method. Split horizon prevents the ACOS device from advertising a route to the neighbor that advertised the same route to the ACOS device.

Syntax `[no] ipv6 rip split-horizon {poisoned | disable | enable}`

Parameter	Description
`poisoned`	Enables advertisement of a route to the neighbor that advertised the route to the ACOS device, but sets the metric value to infinity, thus making the

Parameter	Description
	route advertised by the ACOS device unusable by the neighbor (poisoned reverse). Without this option, advertisement of a route to the neighbor that advertised the route to the ACOS device is not allowed.
disable	Disable the split-horizon method.
enable	Enables split-horizon, but without the poisoned reverse.

Default Split-horizon with poison is enabled.

Mode Interface

ipv6 router isis

Description Configure options for Intermediate System to Intermediate System (IS-IS) on an IPv6 data interface.

Syntax

```
[no] ipv6 router isis [ISO routing area tag name]
```

Default None

Mode Interface

ipv6 router ospf

Description Configure an OSPFv3 area.

Syntax

```
[no] ipv6 router ospf
{
area {num | ipaddr} [tag tag [instance-id num]] |
tag tag area {num | ipaddr} [instance-id num]
}
```

Mode Interface

Usage For OSPFv3, the area tag ID configured on an interface must be the same as the tag ID for the OSPF instance.

ipv6 router rip

Description Configure RIP routing for IPv6.

Syntax

```
[no] ipv6 router rip
```

Mode Interface

ipv6 stateful-firewall

Description Configure stateful firewall direction for this interface.

Syntax

```
[no] ipv6 stateful-firewall {inside | outside [access-list num]}
```

Parameter	Description
inside	Inside (private) interface for the stateful firewall.
outside	Outside (public) interface for the stateful firewall.
access-list	Access list id. You can specify 1-199.

Mode Interface

Example ACOS(config-if:ethernet:1)#ipv6 stateful-firewall outside access-list 1

ipv6 ttl-ignore

Description Configures the device to not decrement TTL field contents for IPv6 traffic passing through. By default TTL decrements for traffic passing through the ACOS device.

Syntax

```
[no] ipv6 ttl-ignore
```

Default Not set

Mode Interface

Example The following example programs the device to not decrement TTL field contents for traffic passing through the ACOS device.

```
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# ipv6 ttl-ignore
ACOS(config-if:ethernet:4)# exit
```

isis authentication

Description Configure authentication for this IS-IS interface.

Syntax

```
[no] isis authentication send-only [level-1 | level-2]
[no] isis authentication mode md5 [level-1 | level-2]
[no] isis authentication key-chain name [level-1 | level-2]
```

Parameter	Description
send-only [**level-1** | **level-2**]	Disables checking for keys in IS-IS packets received by this interface. • **level-1**– Disables key checking only for Level-1 (intra-area) IS-IS traffic. • **level-2**– Disables key checking only for Level-2 (inter-area) IS-IS traffic.
mode md5 [**level-1** | **level-2**]	Enabled MD5 authentication. • **level-1**– Enables MD5 only for Level-1 (intra-area) IS-IS traffic. • **level-2**– Enables MD5 only for Level-2 (inter-area) IS-IS traffic. **NOTE:** The **mode md5** option is not supported in FIPS mode.
key-chain *name* [**level-1** | **level-2**]	Specifies the name of the certificate key chain to use for authenticating IS-IS traffic. • **level-1**– Applies to Level-1 (intra-area) IS-IS traffic. • **level-2**– Applies to Level-2 (inter-area) IS-IS traffic.

Default Clear-text authentication is enabled by default. MD5 authentication is disabled by default. No key chain is set by default. The **send-only** option is disabled by default. For all options that accept the **level-1**, **level-1-2**, or **level-2** keyword, the default is **level-1**.

Mode IS-IS

Usage This command overrides the globally configured authentication settings for the IS-IS instance.

Use the **send-only** option to temporarily disable key checking, then use the **key-chain** option to specify the key chain. To use MD5, use the **md5** option to disable clear-text authentication and enable MD5 authentication. After key-chains are installed on the other IS-IS routers, disable the **send-only** option.

Example The following command disables MD5 authentication for IS-IS on interface VE 2. Clear-text authentication will be used instead.

```
ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# no isis authentication mode md5
```

isis bfd

Description Disable BFD.

Syntax

```
[no] isis bfd disable
```

Default Takes the value from the global BFD configuration.

Mode Interface

isis circuit-type

Description Specify the IS-IS routing level (circuit type) for this interface.

Syntax

```
[no] isis circuit-type [level-1 | level-1-2 | level-2]
```

Specify the IS-IS routing level:

- **level-1** - Intra-area adjacencies are formed
- **level-1-2** - both intra-area and inter-area adjacencies are formed
- **level-2** - Inter-area adjacencies are formed

Default **level-1**

Mode Interface

isis csnp-interval

Description Configure the interval between transmission of complete sequence number PDUs (CSNPs).

Syntax

```
[no] isis csnp-interval seconds [level-1 | level-2]
```

Parameter	Description
seconds	Specifies the number of seconds to wait between transmission of CSNPs. You can specify 0-65535 seconds.
level-1 | **level-2**	Specifies the IS-IS routing level to which the interval setting applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 10 seconds, for both level-1 and level-2

Mode Interface

Usage This command is valid only on broadcast interfaces (network type broadcast).

isis hello

Description Enable padding of IS-IS Hello packets.

Syntax

```
[no] isis hello padding
```

Default Enabled

Mode Interface

Usage When padding is enabled, extra bytes are added to IS-IS Hello packets to make them equal to the MTU size of the interface. This option informs neighbors of the interface's MTU, so that neighbors do not send Hello packets that are longer than the MTU.

isis hello-interval

Description Configure the interval between transmission of IS-IS Hello packets on this interface.

Syntax

```
[no] isis hello-interval seconds [level-1 | level-2]
```

Parameter	Description
seconds	Specifies the number of seconds between transmission of Hello packets to neighbors. You can specify 0-65535 seconds.
level-1 | **level-2**	Specifies the IS-IS routing level to which the interval setting applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 10 seconds, for both level-1 and level-2

Mode Interface

isis hello-interval-minimal

Description Base the hello interval value on the hello multiplier value.

Syntax

```
[no] isis hello-interval-minimal [level-1 | level-2]
```

Parameter	Description
level-1 | **level-2**	Specifies the IS-IS routing level to which the interval setting applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 10 seconds, for both level-1 and level-2

Mode Interface

Usage The **minimal** option bases the hello interval on the hello multiplier, by setting the hold time to 1, and dividing the hold time by the hello multiplier:

```
hello-interval = hold-time % hello-multiplier

hello-interval = 1 % hello-multiplier
```

Related Commands:

- isis hello-multiplier

isis hello-multiplier

Description Configure the multiplier used for calculating the neighbor hold time for Hello packets.

Syntax `[no] isis hello-multiplier num [level-1 | level-2]`

Parameter	Description
num	Specifies the multiplier. You can specify 2-100.
level-1 | **level-2**	Specifies the IS-IS routing level to which the multiplier setting applies.: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 3

Mode Interface

Usage The hold time specifies the maximum number of seconds IS-IS neighbors should allow between Hello packets from this IS-IS interface. If the neighbor does not receive a Hello packet before the hold time expires, the neighbor terminates the adjacency with this IS-IS router on this interface.

To calculate the hold time, IS-IS multiplies the IS-IS hello interval by the multiplier:

```
hello-interval x hello-multiplier = hold-time
```

The hold-time value is included in Hello packets sent to IS-IS neighbors.

NOTE: If the **minimal** option is used with the **isis hello-interval** command, the hold time is set to 1. This overrides the hold time calculated based on the hello-multiplier value.

isis lsp-interval

Description Configure the minimum LSP transmission interval.

Syntax

```
[no] isis lsp-interval ms
```

Replace *ms* with the minimum number of milliseconds IS-IS will wait between transmission of LSPs (1-4294967295).

Default 33 ms

Mode Interface

Usage The LSP transmission interval helps avoid high CPU utilization on IS-IS neighbors during LSP floods, by allowing the neighbors time to send, receive, and process LSPs.

isis mesh-group

Description Configure mesh-group membership to control LSP flooding from this interface.

Syntax

```
[no] isis mesh-group {group-num | blocked}
```

Parameter	Description
group-num	Specifies the mesh group number. You can specify 1-4294967295. LSPs are flooded to all Level-1 or Level-2 IS-IS neighbors (as applicable), except to the neighbors who are in the same mesh group. LSPs are not flooded to the neighbors who are in the same mesh group as this interface.
blocked	Blocks flooding of LSPs on this interface.

Default None

Mode Interface

isis metric

Description Configure the default IS-IS metric (cost) for the interface.

Syntax

```
[no] isis metric num [level-1 | level-2]
```

Parameter	Description
num	Specifies the cost of using this interface as a link in an IS-IS route. You can specify 1-63.
level-1 | **level-2**	Specifies the IS-IS routing level to which the default metric setting applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 10, for Level-1 and Level-2 routing levels

Mode Interface

Usage The default metric is used for SPF calculation. Links with lower metrics are preferred to links with higher metrics.

The default metric is applicable only when the metric-style is narrow.

isis network

Description Configure the network type.

Syntax

```
[no] isis network {broadcast | point-to-point}
```

Parameter	Description
broadcast	The network is a broadcast network.
point-to-point	The network is a point-to-point network.

Default broadcast

Mode Interface

isis password

Description Configure the plain-text password for authentication of Hello packets sent and received on this interface.

Syntax

```
[no] isis password string [level-1 | level-2]
```

Parameter	Description
string	Specifies the password.
level-1 | **level-2**	Specifies the IS-IS routing level to which the password applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default None

Mode Interface

Usage The password is applicable only if the isis authentication type is plain-text.

isis priority

Description Configure this interface's priority for Designated Integrated System (DIS) election.

Syntax

```
[no] isis priority num [level-1 | level-2]
```

Parameter	Description
num	Specify the priority (0-127).
level-1 | **level-2**	Specifies the IS-IS routing level to which the priority applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 64, for Level-1 and Level-2 routing levels

Mode Interface

Usage During DIS election, the IS-IS router with the highest priority is elected as the DIS for the LAN. If more than one IS-IS router has the highest priority, the router that has the IS-IS interface with the highest MAC address is elected as the DIS.

The priority is applicable only if the isis network type is broadcast.

isis restart-hello-interval

Description Configure the amount of time this interface waits for acknowledgement from neighbors of its notification to restart IS-IS, before resending the notification.

Syntax `[no] isis restart-hello-interval seconds [level-1 | level-2]`

Parameter	Description
seconds	Specifies the number of seconds IS-IS waits to receive an acknowledgment of its restart notification. You can specify 1-65535 seconds.
level-1 | **level-2**	Specifies the IS-IS routing level to which the interval applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 3 seconds, for Level-1 and Level-2 routing levels

Mode Interface

Usage To notify its IS-IS neighbors of an intent to restart the IS-IS process, the ACOS device inserts a Restart TLV in IS-IS Hello packets sent to neighbors on this interface. If the an acknowledgement of the restart notification is not received on this interface before the restart hello interval expires, IS-IS resends the notification.

isis retransmit-interval

Description Configure the interval between transmission of LSPs on point-to-point links.

Syntax

```
[no] isis retransmit-interval seconds
```

Replace *seconds* with the number of seconds IS-IS waits before resending an LSP that was dropped (0-65535). Use a value that is greater than the expected round-trip delay between any two routers on the attached network.

Default 5

Mode Interface

Usage The retransmit interval is applicable only if the network type is point-to-point. (See isis network.)

isis wide-metric

Description Configure the length of a wide metric on the interface.

Syntax

```
[no] isis wide-metric num [level-1 | level-2]
```

Parameter	Description
num	Specifies the metric length. You can specify 1-16777214.
level-1 | **level-2**	Specifies the IS-IS routing level to which the metric applies: • **level-1** – Intra-area • **level-2** – Inter-area The default is **level-1**.

Default 10, for Level-1 and Level-2 routing levels

Mode Interface

Usage The wide metric is applicable only if the metric-style is set to wide or transition.

l3-vlan-fwd-disable

Description Disable Layer 3 forwarding between VLANs on tis interface.

Syntax

```
[no] l3-vlan-fwd-disable
```

Default By default, the ACOS device can forward Layer 3 traffic between VLANs.

Mode Interface

Usage This command is applicable only on ACOS devices deployed in gateway (route) mode. If the option to disable Layer 3 forwarding between VLANs is configured at any level, the ACOS device cannot be changed from gateway mode to transparent mode, until the option is removed.

The command is applicable to inbound traffic on the interface.

The command is valid on physical Ethernet interfaces, Virtual Ethernet (VE) interfaces, trunks, and on the lead interface in trunks.

However, if the command is configured on a physical Ethernet interface, that interface cannot be added to a trunk or VE.

If the command is used on a trunk or VE and that trunk or VE is removed from the configuration, the command is also removed from all physical Ethernet interfaces that were members of the trunk or VE. Likewise, if a VLAN is removed, the command is removed from any physical Ethernet interfaces that were members of the VLAN.

Related Commands:

- show slb switch

lldp enable

Description Configure this interface to send only, receive only, or send and receive LLDP data packets.

Specify **rx** to configure the interface to only receive LLDP data packets; specify **tx** to configure the interface to only send LLDP data packets. If neither is specified, the interface can both receive and send LLDP data packets.

Syntax

```
[no] lldp enable [rx] [tx]
```

Default Not enabled.

Mode Port configuration mode

lldp notification

Description Configure this port to send notifications.

Syntax

```
[no] lldp notification enable
```

Default Not enabled.

Mode Interface

lldp tx-dot1-tlvs

Description The TLVs VLAN name and link-aggregation are dictated by 802.1ab Annex E.

Syntax

```
[no] lldp tx-dot1-tlvs [vlan] [link-aggregation]
```

Parameter	Description
`vlan`	Assign a name to the VLAN and map the VLAN ID to the VLAN.
`link-aggregation`	Link-aggregation TLV, dictated by 802.1ab 2005 and 802.1ab 2009.

Default Since 802.1ab 2009 and 802.1ab2005 are inherently different, some older devices do support these TLVs by default. The TLVs will not automatically be included in the transmitted frame.

Mode Interface

lldp tx-tlvs

Description Configure the transmission TLV packets to exclude. All basic TLVs will be included by default.

Syntax

```
[no] lldp tx tlvs exclude {
  management-address |
  port-description |
  system-capabilities |
  system-description |
```

```
  system-name
}
```

Default Not enabled.

Mode Interface

load-interval

Description Change the interval for utilization statistics for the interface.

Syntax

```
[no] load-interval seconds
```

You can specify 5-300 seconds.

You must specify the amount in 5-second intervals. For example, 290 and 295 are valid interval values. However, 291, 292, 293, and 294 are not valid interval values.

Default 300 seconds

Mode Interface

Usage This command applies only to data interfaces.

Example The following command changes the utilization statistics interval for Ethernet interface 1 to 200 seconds:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# load-interval 200
```

Related Commands:

- show interfaces
- show statistics

lw-4o6

Description Configure an LW-4over6 interface.

Syntax

```
[no] lw-4o6 {inside | outside}
```

Parameter	Description
`inside`	Configure an LW-4over6 inside interface.
`outside`	Configure an LW-4over6 outside interface.

Mode Interface

map-inside

Description This command enables MAP on the inside interface connected to the CEs and the private IPv6 network.

Syntax
```
[no] map inside
```

Default Disabled.

Mode Interface configuration mode.

map outside

Description This command enables MAP on the outside interface connected to the public IPv4 network.

Syntax
```
[no] map outside
```

Default Disabled.

Mode Interface configuration mode.

media-type-copper

Description Configure a 40G port if you want to use a copper 40G DAC cable.

This command is only available on devices with 40G interfaces.

Syntax
```
[no] media-type-copper
```

Default 40G ports on ACOS devices are configured to use fiber cables by default.

Mode Interface

monitor

Description Configure an Ethernet data interface to send a copy of its traffic to another Ethernet data interface.

Prerequisite Configure a mirror port to accept the copied (mirrored) traffic. All mirrored traffic for the directions you specify goes to this port.

NOTE: Only one mirror port is supported.

Syntax

```
[no] monitor {both | input | output} [vlan vlan-id]
```

Parameter	Description
both	Send a copy of both inbound and outbound traffic to the mirror port. The mirror port must have already been configured to send both inbound and outbound mirrored traffic from this monitored port. For example: `ACOS(config)# mirror-port 1 ethernet 1 both`
input	Send inbound traffic only to the mirror port. The mirror port must have already been configured to send inbound mirrored traffic from this monitored port. For example: `ACOS(config)# mirror-port 2 ethernet 2 input`
output	Send outbound traffic only to the mirror port. The mirror port must have already been configured to accept outbound mirrored traffic from this monitored port. For example: `ACOS(config)# mirror-port 3 ethernet 3 output`
vlan *vlan-id*	If applicable, specify the VLAN to which the monitored port belongs.

Default By default, no traffic is mirrored.

Mode Interface

Example The following commands enable monitoring of input traffic on Ethernet port 5, and enable the monitored traffic to be copied ("mirrored") to Ethernet port 3:

```
ACOS(config)# mirror-port 2 ethernet 3
ACOS(config)# interface ethernet 5
ACOS(config-if:ethernet:5)# monitor input 2
```

mtu

Description Change the Maximum Transmission Unit (MTU) for an Ethernet interface.

Syntax

```
[no] mtu bytes
```

Replace *bytes* with the largest packet size that can be forwarded out the interface (434-1500).

NOTE: See Usage section below for details on jumbo frame support.

Default 1500 bytes

Mode Interface

Usage This command applies to the Ethernet data interfaces.

If the ACOS device needs to forward a packet that is larger than the MTU of the ACOS egress interface to the next hop, but the Do Not Fragment bit is set in the packet, the ACOS device drops the packet and sends an ICMP Destination Unreachable code 4 (Fragmentation required, and DF set) message to the sender.

To display a counter of how many outbound packets have been dropped because they were longer than the outbound interface's MTU, use the following command:

```
show slb switch [detail | ethernet port-num [detail]]
```

The counter is labeled "MTU exceeded Drops". The counter includes packets that had the Do Not Fragment bit set and packets that did not have the bit set.

You can enable jumbo support on a global basis. In this case, the MTU is not automatically changed on any interfaces, but you can increase the MTU on individual interfaces.

- On FTA models, you can increase the MTU on individual Ethernet interfaces up to 12000 bytes.
- On non-FTA models, you can increase the MTU on individual Ethernet interfaces up to 9216 bytes.

name

Description Assign a name to the interface.

Syntax

```
[no] name string
```

Replace *string* with the name for the interface, 1-63 characters.

Default None

Mode Interface

Usage This command applies to physical and virtual Ethernet data interfaces, tunnels, and trunks. This command does not apply to the management interface.

Example The following commands assign the name "WLAN-interface" to an interface and show the result:

```
ACOS(config)# interface ve 1
ACOS(config-if:ve:1)# name WLAN-interface
ACOS(config-if:ve:1)# show ip interfaces
Port IP              Netmask      PrimaryIP   Name
-----------------------------------------------------------
mgm  192.168.20.136  255.255.255.0   Yes
ve1  192.168.217.1   255.255.255.0   Yes     WLAN-interface
ve2  50.50.50.1      255.255.255.0   Yes
```

ports-threshold

Description Configures the minimum port threshold for a trunk.

Syntax

```
[no] ports-threshold number-of-ports
[timer seconds [do-auto-recovery]]
```

Parameter	Description
number-of-ports	Minimum number of ports that must be up in order for the trunk to remain Up. If the number of Up ports falls below the configured threshold, the ACOS device automatically disables the trunk's member ports. You can specify a range of 2-8.
timer *seconds* [**do-auto-recovery**]	In the `do-auto-recovery` mode, when any member port in the trunk comes Up, a timer is started. Once the timer expires, • if the number of member ports that are Up exceeds the configured ports threshold, the trunk is brought Up. • if the number of member ports that are Up is below the configured ports threshold, the trunk is brought Down. Without the `do-auto-recovery` option, when the trunk is manually configured to be brought Up, a timer is started. Once the timer expires, • if the number of member ports that are Up exceeds the configured ports threshold, the trunk is brought Up. • if the number of member ports that are up is below the configured ports threshold, the trunk is brought Down. You can set the ports-threshold timer in a range of 1-300 seconds. The default value is 10 seconds.

Mode Interface

Usage This command applies only to trunk interfaces.

remove-vlan-tag

Description Remove the VLAN tag from packets to ensure that packets going out of the interface will be untagged.

NOTE: This command is not available on non-FTA platforms, and is also not available on the A10 Thunder Series 3230S(S), 3430(S), and 5330(S) platforms.

Syntax

```
[no] remove-vlan-tag
```

Default Disabled

Mode Interface

Example Ensure packets going out of ethernet interface 2 are untagged:

```
ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# remove-vlan-tag
```

snmp-server

Description Specify a data interface to use as the source interface for SNMP traps.

Syntax

```
[no] snmp-server trap-source
```

Default Management interface

Mode Interface

Usage Select a data interfaces from which to send SNMP traps. The interface can be any of the following types:

- Ethernet
- VLAN / VE
- Loopback

When the ACOS device sends an SNMP trap from the specified data interface, the “agent-address” in the SNMP trap is the data interface’s IP address.

Implementation Details:

- This feature does not support IPv6.
- This feature supports SNMPv1 but not SNMPv2c or SNMPv3.

Example The following command attempts to set a loopback interface as the SNMP trap source. However, the feature has already been enabled on

Ethernet port 1, and only one interface can be enabled for SNMP traps, so this example shows that the existing trap source will be overwritten with the new one:

```
ACOS(config)# interface loopback 1
ACOS(config-if:loopback:1)# snmp-server trap-source
The trap source already exists for interface eth1. Do you want
to overwrite? [yes/no]:yes
ACOS(config-if:loopback:1)#
```

traffic-distribution-mode

Description Distributes the traffic to a specific destination based on the mode selected.

Syntax

```
[no] traffic-distribution-mode [ sip | dip | l3-lookup |
primary | blade | l4-src-port | l4-dst-port ]
```

Command	Description
sip	Distribute the traffic evenly to the Multi-PUs (PU1 and PU2) based on the source IP address.
dip	Distribute the traffic evenly to the Multi-PUs (PU1 and PU2) based on the destination IP address.
l3-lookup	Specify this distribution mode for a DMZ-facing interface to distribute traffic evenly across Multi-PUs based on the result of an L3 lookup, populated via class-list of client IP addresses. The class list of client IP addresses can be configured using the fw client class-list command.
primary	Distribute the traffic to the primary (master) unit.
blade	Distribute the traffic to the secondary (blade) unit.
l4-src-port	Distribute the traffic to the Multi-PUs based on the layer 4 source port.
l4-dst-port	Distributes the traffic to the Multi-PUs based on the layer 4 destination port.

Mode VLAN or Interface

Usage This command is used to define the traffic distribution mode.

Example The following command sets the traffic distribution mode as **sip/dip** in VLAN:

```
ACOS(config)# vlan 90
ACOS(config-vlan:90)# traffic-distribution-mode sip
ACOS(config)# vlan 91
ACOS(config-vlan:90)# traffic-distribution-mode dip
```

Example The following command sets the traffic distribution mode as **l3-lookup** in VLAN:

```
ACOS(config)# vlan 211
ACOS(config-vlan:211)# tagged ethernet 13
ACOS(config-vlan:211)# router-interface ve 211
ACOS(config-vlan:211)# traffic-distribution-mode l3-lookup
```

Example The following command sets the traffic distribution mode as **sip or dip** in the Interface ethernet:

```
ACOS(config)# interface ethernet 6
ACOS(config-if:ethernet:6)# enable
ACOS[ssli_in](config-if:ethernet:6)# traffic-distribution-mode
dip
ACOS(config)# interface ethernet 7
ACOS(config-if:ethernet:7)# enable
ACOS(config-if:ethernet:7)# traffic-distribution-mode sip
```

Related Commands:

- vlan
- interface
- system chassis-port-split
- odd-even-nat-enable

trunk-group

Description Add the interface to a trunk group.

Syntax

```
[no] trunk-group TrunkID [static | lacp | lacp-udld]
```

Parameter	Description
TrunkID	Trunk number, 1-4096. **NOTE:** the maximum number of trunk instances that can be configured on an interface is 16; each TrunkID specified is mapped to the next available instance (1-16).
static	Adds the interface to a static trunk.
lacp	Adds the interface to a dynamic trunk.
lacp-udld	Adds the interface to a dynamic trunk that uses Unidirectional Link Detection.

Default **static**

Mode Interface

Usage Use this command on each Ethernet data port you want to add to the trunk. When finished, use the **interface trunk** *TrunkID* command to access the configuration level for the trunk interface.

For more information, refer 'Link Trunking' in the *Network Configuration Guide*.

virtual-wire

Description Enable ethernet as a virtual wire interface. The virtual wire is created with ID number only. You can also specify options to update the L2 information.

Syntax

```
[no] virtual-wire [ update-l2-info vlan-learning {enable | disable} mac-learning {enable | disable} ]
```

Parameter	Description
update-l2-info	Specify this option to update the L2 information of the existing session if it has changed. L2 information includes the VLAN tag and MAC address. You need to specify the options **vlan-**

Parameter	Description
	learning and **mac-learning** to select the type of information that needs to be updated.
vlan-learning {enable | disable}	Enable or disable this option that checks and updates VLAN tags.
mac-learning {enable | disable}	Enable or disable this option that checks and updates MAC addresses.

Default None

Mode Interface

Usage This command applies to ethernet and trunks interfaces.

NOTE: Once the interface is specified with **update-l2-info**option, the session triggered by this interface will use the latest information to send out packets no matter which learning mode is used.

Example The following command enable simple virtual wire interface:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# virtual-wire
```

Example The following command demonstrates **update-l2-info** usage:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# virtual-wire update-l2-info vlan-
learning disable mac-learning enable
```

ip

Description Configure global IP settings.

ip access-list

Description Configures an IPv4 access control list (ACL).

Syntax

```
[no] ip access-list  acl-name
```

Replace *acl-name* with the name of the IP ACL, 1-16 characters.

This command changes the CLI to the configuration level for the specified IPv4 ACL, where the following commands are available:

```
{
[sequence-number]
  {[remarkstring] |
  [deny | permit | l3-vlan-fwd-disable]}
    {traffic-type}
      {traffic-source}
        {traffic-destination}
          {more-options}
}
```

Match Option	Description
sequence-number	Sequence number of this rule in the ACL. You can use this option to resequence the rules in the ACL.
remark *string*	Adds a remark to the ACL (1-63 characters). The remark appears at the top of the ACL when you display it in the CLI. To use blank spaces in the remark, enclose the entire remark string in double quotes. The ACL must already exist before you can configure a remark for it. An ACL and its individual rules can have multiple remarks.
deny | **permit** | **l3-vlan-fwd-disable**	Specify the action to take for traffic that matches the ACL: • **deny** - Drops any traffic that matches the ACL applied to interfaces or used for management access.

Match Option	Description
	• **permit** - Allows any traffic that matches the ACL applied to interfaces or used for management access. For ACLS used for IP source NAT, this option s pecifies the inside host addresses to be translated into external addresses. **NOTE:** If you are configuring an ACL for source NAT, use the **permit** action. For ACLs used with source NAT, the **deny** action does not drop traffic, it simply does not use the denied addresses for NAT translations. • **l3-vlan-fwd-disable** - Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
traffic-type	Specifies the type of traffic to match: • **geo-location** – Matches on geo-location name. • **icmp** [**type** {*type-option*} [**code** {**any-code** | *code-num*}]] – Matches on ICMP traffic. • **ip** – Matches on any type of IP traffic. • **object-group** *group-name* – Matches on the values in the specified service object group. • **tcp** – Matches on TCP traffic. • **udp** – Matches on UDP traffic.
traffic-source	Specifies the source address(es) on which to match: • **any** – The ACL matches on all source IP addresses. • **host** *host-src-ipaddr* – The ACL matches only on the specified host IP address. • *net-src-ipaddr* {*filter-mask* | **/***mask-length*} –

Match Option	Description
	The ACL matches on any host in the specified subnet. The filter-mask specifies the portion of the address to filter: ◦ Use 0 to match. ◦ Use 255 to ignore. For example, the following *filter-mask* filters on a 24-bit subnet: 0.0.0.255 Alternatively, you can use *mask-length* to specify the portion of the address to filter. For example, you can specify "/24" instead "0.0.0.255" to filter on a 24-bit subnet. • **object-group** *group-name* – Matches on the addresses in the specified network object group.
eq *src-port* | **gt** *src-port* | **lt** *src-port* | **range** *start-src-port end-src-port*	These options are available for both TCP or UDP only; they specify the source protocol ports on which to match: • **eq** *src-port* – The ACL matches on traffic from the specified source port. • **gt** *src-port* – The ACL matches on traffic from any source port with a higher number than the specified port. • **lt** *src-port* – The ACL matches on traffic from any source port with a lower number than the specified port. • **range***start-src-port end-src-port* – The ACL matches on traffic from any source port within the specified range.
traffic-destination	Specifies the destination address(es) on which to match. (The options are the same as those for source address.)

Match Option	Description
more-options	Specifies additional match criteria: • **fragments** – Matches on packets in which the More bit in the header is set (1) or has a non-zero offset. • **vlan** *vlan-id* – Matches on the specified VLAN. VLAN matching occurs for incoming traffic only. • **dscp***num* – Matches on the 6-bit Diffserv value in the IP header, 1-63. • **established** – Matches on TCP packets in which the ACK or RST bit is not set. This option is useful for protecting against attacks from outside. Since a TCP connection from the outside does not have the ACK bit set (SYN only), the connection is dropped. Similarly, a connection established from the inside always has the ACK bit set. (The first packet to the network from outside is a SYN/ACK.) • **log** [**transparent-session-only**] – Configures the ACOS device to generate log messages when traffic matches the ACL. The transparent-session-only option limits logging for an ACL rule to creation and deletion of transparent sessions for traffic that matches the ACL rule.

Mode Configuration mode.

Usage The support for named IPv4 ACLs supplements the support for IPv4 ACLs configured by ID. You can use a named IPv4 ACL in any place a standard or extended IPv4 ACL is supported. In the CLI, use the name option in front of the IPv4 ACL name.

Example The following commands configure a named, extended IPv4 ACL called "Deny-Rules" to deny traffic sent from subnet 10.10.10.x to 10.10.20.5:80, and apply the ACL to inbound traffic received on Ethernet interface 7:

```
ACOS(config)# ip access-list Deny-Rules
ACOS(config-ext-access-list:Deny-Rules)# deny tcp 10.10.10.0
0.0.0.255 10.10.20.5 /32 eq 80
ACOS(config-ext-access-list:Deny-Rules)# exit
ACOS(config)# interface ethernet 7
ACOS(config-if:ethernet:7)# access-list name Deny-Rules in
```

Related Commands:

- object-group service

ip address

Description Configures the global IP address of the ACOS device, when the device is deployed in transparent mode (Layer 2 mode).

Syntax `[no] ip address ipaddr {subnet-mask | /mask-length}`

Default None.

Mode Configuration mode

Usage This command applies only when the ACOS device is deployed in transparent mode. To assign IP addresses to individual interfaces instead (gateway mode), use the **ip address** command at the interface configuration level. (See ip address.)

NOTE: The IPv4 link-local address 169.254.x.x/16 is not supported.

If the ACOS device is a member of an aVCS, use the **device-context** command to specify the device in the Multi-PU platforms to which this command must apply.

Loopback Interface Support for OSPF

If an IP address is configured on a loopback interface, and the address is in a subnet that is also configured as an OSPF network subnet, the loopback interface is automatically included in the OSPF subnet.

The ACOS device's table of OSPF interfaces will include the loopback interface. Likewise, the ACOS device will include the loopback interface in link-state advertisements sent to neighbor OSPF routers.

Multiple OSPF Networks on the Same Interface Not Supported

The ACOS device does not support multiple OSPF networks on a data interface. One OSPF network configuration can enable at most one network per interface.

For example, assume a data port has 3 IP addresses configured that belong to 3 separate subnets, S1, S2, and S3. If you configure network S4 with area A.B.C.D, and S4 contains S1, S2, and S3, then only S1 will be running OSPF. S2 and S3 will not be known to other OSPF routers.

To work around this limitation, enable OSPF redistribution of directly connected routes so that OSPF will redistribute S2 and S3 via the network running on S1.

Example The following command configures global IP address 10.10.10.4/24:

```
ACOS(config)# ip address 10.10.10.4 /24
```

ip anomaly-drop

Description Enable filtering for IP packets that exhibit predictable, well-defined anomalies. You can enable filtering for the following types of IP anomalies:

Syntax

```
[no] ip anomaly-drop {parameter} variable if applicable
```

Parameter	Description
bad-content	Bad content threshold. You can specify a value of 1-127.
drop-all	Drop all IP anomaly packets.
frag	Drop all fragmented packets.

Parameter	Description
ip-option	Drop packets with IP options.
land-attack	Drop IP packets with the same source and destination addresses.
out-of-sequence	Out of sequence packet threshold. You can specify a value of 1-127.
packet-deformity	Drop packets with deformity. You can specify layer-3 or layer-4.
ping-of-death	Drop oversize ICMP packets.
security-attack	Drop packets causing a security attack. You can specify layer-3 or layer-4.
tcp-no-flag	Drop TCP packets with no flag.
tcp-syn-fin	Drop TCP packets with both syn and fin flags set.
tcp-syn-frag	Drop fragmented TCP packets with a syn flag set.
zero-window	Zero window size threshold.

Default All options are disabled by default.

Mode Configuration mode

Example The following is the configuration example:

```
ACOS(config)# ip anomaly-drop security-attack layer-3
```

ip as-path

Description Configure an AS-path list for BGP.

Syntax

```
[no] ip as-path access-list regular-expression {deny | permit}
```

Parameter	Description
regular-expression	Access list name.
deny | **permit**	Action to perform on matching entries.

Default None

Mode Configuration mode

ip community-list

Description Specify BGP community attributes.

Syntax

```
[no] ip community-list num
{deny | permit}
[community-number]
[local-AS]
[no-advertise]
[no-export]
```

Syntax

```
[no] ip community-list {expanded | standard}  list-name
{deny | permit}
[community-number]
[1-4294967295]
[AA:NN]
[internet]
[local-AS]
[no-advertise]
[no-export]
```

Parameter	Description
num	List number.
{**expanded** | **standard**} *list-name*	List type and name.
deny | **permit**	Action to perform for matching communities.
community-number	Community number.
1-4294967295	Number of routes that can be advertised.

Parameter	Description
AA:NN	Format of the routes to be advertised.
internet	Advertises routes on the internet.
local-AS	Advertises routes only within the local Autonomous System (AS), not to external BGP peers.
no-advertise	Does not advertise routes.
no-export	Does not advertise routes outside the AS boundary.

Default None

Mode Configuration mode

Example Example configuration:

```
ACOS(config)# ip community-list standard list-name permit 10
no-advertise
```

ip large-community-list

Description Configures a large community list for BGP.

Syntax

```
[no] ip community-list {expanded | standard}  list-name  | num
<1-99> or <100-199>}
{deny | permit}
[community-number XX:YY:ZZ]
```

Parameter	Description
{**expanded** | **standard**} *list-name*	List type and name.
num	List number.
deny | **permit**	Action to perform for matching communities.
community-number	Community number in XX:YY:ZZ fromat.

Default None

Mode Configuration mode

Example This is an example of configuration of a large community list:

```
ACOS(config)# ip large-community-list standard examplelistname
permit 123456:12345:1234567
```

ip default-gateway

Description Specify the default gateway to use to reach other subnets, when the ACOS device is deployed in transparent mode (Layer 2 mode).

Syntax

```
[no] ip default-gateway ipaddr
```

Default None.

Mode Configuration mode

Usage This command applies only when the ACOS device is used in transparent mode. If you instead want to use the device in gateway mode (Layer 3 mode), configure routing.

To configure the default gateway for the out-of-band management interface, use the **interface management** command to go to the configuration level for the interface, then enter the **ip default-gateway** command. (See ip default-gateway.)

If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the Multi-PU platforms to which this command must apply.

Example The following command configures an ACOS device deployed in transparent mode to use router 10.10.10.1 as the default gateway for data traffic:

```
ACOS(config)# ip default-gateway 10.10.10.1
```

ip dmz

Description Enable Demilitarized Zone (DMZ) facing interface for IPv4 or IPv6 traffic.

Syntax

```
[no] ip dmz
```

Default Not enabled

Mode Interface

Usage The **ip dmz** command can be configured under **interface ethernet** as well as **interface ve**.

NOTE: The interface tag **ip dmz** cannot be configured with **ip client/ip server/ip nat inside**. However, it can be configured along with **ip nat outside**.

Example Configure the DMZ-facing interface under **interface ethernet** using the following command:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# ip address 10.1.1.47 255.255.255.0
ACOS(config-if:ethernet:1)# ip dmz
```

Example Configure the DMZ-facing interface under **interface ve** using the following command:

```
ACOS(config)# interface ve 3250
ACOS(config-if:ve:3250)# ip address 10.1.1.47 255.255.255.0
ACOS(config-if:ve:3250)# ip dmz
```

- ip client
- ip server
- ip nat

For more information, refer to the *Firewall Configuration guide*.

ip dns

Description Configure DNS servers and the default domain name (DNS suffix) for hostnames on the ACOS device.

Syntax

```
[no] ip dns {primary | secondary} ipaddr
[no] ip dns suffix string
```

Default None

Mode Configuration mode

Usage This command applies to transparent mode and gateway mode.

This command can be used in both shared and L3V partitions.

Example The following command sets primary DNS server 20.20.20.5:

```
ACOS(config)# ip dns primary 20.20.20.5
```

ip extcommunity-list

Description Configure an extended community list for BGP.

Syntax

```
[no] ip extcommunity-list num
{deny | permit}
{rt | soo {AS-num:nn | ipaddr:nn}}
```

Syntax

```
[no] ip extcommunity-list
{expanded | standard} list-name
{deny | permit}
{rt | soo {AS-num:nn | ipaddr:nn}}
```

Parameter	Description
num	List number.
{**expanded** | **standard**} *list-name*	List type and name.
deny | **permit**	Action to perform for matching communities.
rt | **soo** {*AS-num:nn* | *ipaddr:nn*}	Community type and ID: • **rt** – Route-target extended community. • **soo** – Site-of-origin extended community.

Default None

Mode Configuration mode

```
ACOS(config)# ip extcommunity-list standard list-name permit
soo 10:20
```

ip frag buff

Description Maximum buffer size used for fragmentation.

Syntax

```
[no] ip frag buff num
```

Replace *num* with the maximum number of buffers the ACOS device will allow for fragmentation sessions. You can specify 10000-3000000 (3 million). The specified maximum applies to both IPv4 and IPv6.

Default The default range on 64-bit ACOS models is 5% of total buffers

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **`device-context`** command to specify the device in the chassis to which this command must apply.

ip frag cpu-threshold

Description Set the CPU usage threshold at which to stop processing fragmented packets.

Syntax

```
[no] ip frag cpu-threshold high max-use low min-use
```

Parameter	Description
max-use	The max CPU usage percentage allowed, specified as a number between 0 and 100. When CPU usage exceeds this threshold, the CPU will stop processing fragments.
min-use	The minimum CPU usage percentage that needs to be maintained before the CPU starts processing fragments again. This value is specified as a number between 0 and 100.

Default The default high is 75% and the default low is 60%.

Mode Configuration mode.

ip frag max-packets-per-reassembly

Description Maximum number of fragmented packets allowed per reassembly(0 is unlimited) (default 0)

Syntax

```
[no] ip frag max-packets-per-assembly num
```

Replace *num* with the maximum number of fragmented packets the ACOS device will allow per reassembly. You can specify 2-16.

Default 0

Mode Configuration mode

ip frag max-reassembly-sessions

Description Configure the IP fragment queue size.

Syntax

```
[no] ip frag max-reassembly-sessions num
```

Replace *num* with the maximum number of simultaneous fragmentation sessions the ACOS device will allow. You can specify 1-200000. The specified maximum applies to both IPv4 and IPv6.

Default 100000

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS, use the **device-context** command to specify the device in the Multi-PU platforms to which this command must apply.

ip frag timeout

Description Configures the timeout for IP packet fragments.

Syntax

```
[no] ip frag timeout ms
```

Replace *ms* with the number of milliseconds (ms) the ACOS device buffers fragments for fragmented IP packets. If any fragments of an IP packet do not arrive within the specified time, the fragments are discarded and the packet is not re-assembled. You can specify 4-65535 ms, in 10-ms increments.

Default 60000 ms

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS, use the **device-context** command to specify the device in the Multi-PU platforms to which this command must apply.

ip icmp disable

Description Disables ICMP messages.

Syntax

```
[no] ip icmp disable {redirect | unreachable}
```

Parameter	Description
redirect	Disables sending of ICMP Redirect messages.
unreachable	Disables sending of ICMP Destination Unreachable messages.

Default Both types of ICMP messages are enabled.

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command disables sending of IPv4 ICMP Redirect messages:

```
ACOS(config)# ip icmp disable redirect
```

ip-list

Description Configure an IP list.

Syntax

```
[no] ip-list name
```

Replace *name* with the name of the IP list, 1-63 characters.

Default None

Mode Configuration mode

ip map-list

Description Configure IP Map List name.

Syntax

```
[no] ip map-list name
```

Replace *name* with the name of the IP Map List. You can specify 1-63.

Default Not set

Mode Configuration mode

ip mgmt-traffic

Description Allows a loopback interface IP address to be used as the source interface for management traffic originated by the ACOS device.

Syntax

```
[no] ip mgmt-traffic
{all | ftp | ntp | rcp | snmp | ssh | syslog | telnet | tftp |
web}
source-interface loopback num
```

To apply the command only to a specific type of traffic (SNMP, NTP, and so on), use the option for that traffic type. To apply the command to all management traffic types, use the **all** option.

Default Not set

Mode Configuration mode

Usage Notes about the implementation of this command:

- Loopback interface IP address – The loopback interface you specify when configuring this feature must have an IP address configured on it. Otherwise, this feature does not take effect.
- Management interface – If use of the management interface as the source for management traffic is also enabled, the loopback interface takes precedence over the management interface. The loopback interface's IP address will be used instead of the management interface's IP address as the source for the management traffic.
- Likewise, the **use-mgmt-port** option has no effect.
- Ping traffic – Configuration for use of a loopback interface as the source for management traffic does not apply to ping traffic. By default, ping packets are sourced from the best interface based on the route table. You can override the default interface selection by specifying a loopback or other type of interface as part of the **ping** command.
- Layer 2/3 Virtualization – This feature is supported only for loopback interfaces that belong to the shared partition. When this

feature is configured, management traffic initiated from a private partition will use the IP address of the specified loopback interface as the source address, and will use the shared partition's data routing table to select the outbound interface.

Limitations

- The current release has the following limitations related to this feature:
- Floating loopback interfaces are not supported.
- IPv6 interfaces are not supported.
- aVCS is not supported.

Example The following commands configure an IP address on loopback interface 2:

```
ACOS(config)# interface loopback 2
ACOS(config-if:loopback:2)# ip address 10.10.10.66 /24
ACOS(config-if:loopback:2)# exit
```

Example The following command configures the ACOS device to use loopback interface 2 as the source interface for management traffic of all types listed above:

```
ACOS(config)# ip mgmt-traffic all loopback 2
```

ip nat alg dns

Description Disables or enables NAT Application-Layer Gateway (ALG) support for the DNS.

Syntax

```
ip nat alg dns {enable | disable}
```

Default Enabled

Mode Configuration mode

Example The following command disables the DNS NAT ALG.

```
ACOS(config)# ip nat alg dns disable
```

ip nat alg pptp

Description Disables or re-enables NAT Application-Layer Gateway (ALG) support for the Point-to-Point Tunneling Protocol (PPTP). This feature enables clients and servers to exchange Point-to-Point (PPP) traffic through the ACOS device over a Generic Routing Encapsulation (GRE) tunnel. PPTP is used to connect Microsoft Virtual Private Network (VPN) clients and VPN hosts.

Syntax

```
ip nat alg pptp {enable | disable}
```

Default Enabled

Mode Configuration mode

Usage NAT ALG for PPTP has additional configuration requirements. For more information, see *System Configuration and Administration Guide*.

ip nat icmp

Description Configure NAT ICMP settings.

Syntax

```
[no] ip nat icmp { always-source-nat-errors | respond-to-ping
}
```

Parameter	Description
`always-source-nat-errors`	Enable NAT for ICMP messages from inside routers. By default, source IP addresses of ICMP error messages sent by inside routers are not translated into NAT addresses.
`respond-to-ping`	Enable ping replies from NAT pool addresses. By default, ping requests sent to LSN NAT pool addresses are dropped.

Default Disabled

Mode Configuration mode

ip nat inside source

Description Configure inside Network Address Translation (NAT).

Syntax

```
[no] ip nat inside source {
class-list name |
list acl-name pool pool-or-group-name
  [msl seconds] [respond-to-user-mac] |
static inside-ipaddr nat-ipaddr
  [disable | enable] [vrid num]}
```

Parameter	Description
class-list *name*	Specifies a class list. Entries in the class list map internal IP addresses to IP NAT pools.
list *acl-name*	Specifies an ACL that matches on the inside addresses to be translated.
pool *pool-or-group-name* [**msl** *seconds*] [**respond-to-user-mac**]	Dynamically assigns addresses from a range defined in a pool or pool group. The `msl` option sets the TCP Maximum Segment Life (MSL) for source- NAT connections that use the specified pool or pool group. This option is useful for NAT connections to devices with older TCP/IP stacks, where the MSL is up to 2 minutes, resulting in a wait of up to 240 seconds (4 minutes) after a FIN before the endpoint can enter a new connection. You can set the MSL to 1-1800 seconds. The `respond-to-user-mac` option causes existing connections to follow the active ACOS device to use the inside client's MAC address, instead of the routing table, to select the next hop for the reply. **NOTE:** This option is valid only for the current session. After the client's MAC address expires, the ACOS device will use the routing table to select the next hop. If the session has traffic from the inside client, the ACOS device will learn the inside client's MAC address again.
static *inside-ipaddr*	Statically maps the specified inside address to a specific NAT address.

Parameter	Description
nat-ipaddr	
disable | **enable**	Disables or re-enables the static mapping.
vrid *num*	VRRP-A VRID

Default None

Mode Configuration mode

Usage For Static NAT mappings, the following limitations apply:

- Only the Static NAT + FTP ALG is supported.
- Syn-cookies are not supported.
- VRRP-A session synchronization is not supported. However, sessions will not be interrupted by failover.

Example The following command configures static inside NAT translation of 10.10.10.55 to 192.168.20.44:

```
ACOS(config)# ip nat inside source static 10.10.10.55
192.168.20.44
```

Related Commands:

- access-list (standard)
- access-list (extended)

ip nat pool

Description Configure a named set of IP addresses for use by NAT.

Syntax

```
[no] ip nat pool pool-name
start-ipaddr end-ipaddr
netmask {subnet-mask | /mask-length}
[gateway ipaddr]
[ip-rr]
[port-overload]
[scaleout-device-id device-id]
[vrid num]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | **/***mask-length*}	Network mask for the IP addresses in the pool.
gateway *ipaddr*	Default gateway to use for NATted traffic.
ip-rr	Uses pool IP addresses in round robin fashion. Without this option, IP address selection from a NAT pool depends on the incoming tuple and the usage of the NAT pool.
port-overload	Nat Pool Port overload. To process more than 65535 concurrent connections by supporting that a given SNAT address can continue to use the same source port as long as the remote socket is unique. **NOTE:** The `port-overload` option can only be used when using the NAT pool with reverse proxy, and it can be used in the SNAT pool bound to a virtual port.
scaleout-device-id *device-id*	Configure the Scale Out device ID to which this IP NAT pool will be bound (1-64).
vrid *num*	VRRP-A VRID. In the shared partition, you can specify 1-31 or **default**. In private partitions, you can specify **default**.

Default None.

Mode Configuration mode

Usage The pool can be used by other ip nat commands. The IP addresses must be IPv4 addresses.

When you use the **gateway** option, the gateway you specify is used as follows:

- For forward traffic (traffic from a client to a server), the NAT gateway is used if the source NAT address (the address from the pool) and the server address are not in the same IP subnet.
- On reverse traffic (reply traffic from a server to a client), the NAT gateway is used if all the following conditions are true:
  - The session is using translated addresses (is source NATted).
  - The source protocol port is in the source NAT subnet.
  - The destination is not in the source NAT subnet.

NOTE: The **gateway** option works only when the **allow-in-gateway-mode** option is enabled in snat-gwy-for-l3 command available under SLB common configuration mode.

For conditions under which the NAT gateway is needed, if no NAT gateway is configured, the ACOS device uses the default gateway configured for the ACOS device's other traffic instead.

Example The following command configures an IP address pool named "pool1" that contains addresses from 30.30.30.1 to 30.30.30.254:

```
ACOS(config)# ip nat pool pool1 30.30.30.1 30.30.30.254
netmask /24
```

ip nat pool-group

Description Configure a set of IP pools for use by NAT. Pool groups enable you to use non-contiguous IP address ranges, by combining multiple IP address pools.

Syntax

```
[no] ip nat pool-group pool-group-name [vrid num]
```

Parameter	Description
pool-group-name	Name of the pool group.
vrid *num*	VRRP-A VRID.

This command changes the CLI to the configuration level for the specified pool group, where the following command is available:

member *pool-name*

Replace *pool-name* with the name of a configured IP address pool.

Default None.

Mode Configuration mode

Usage To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

For SLB, a pool group can contain up to 5 pools. Pool group members must belong to the same protocol family (IPv4 or IPv6). A pool can be a member of multiple pool groups.

If a pool group contains pools in different subnets, the ACOS device selects the pool that matches the outbound subnet. For example, if there are two routes to a given destination, in different subnets, and the pool group has a pool for one of those subnets, ACOS selects the pool that is in the subnet for the outbound route.

The ACOS device selects the pool whose addresses are in the same subnet as the next-hop interface used by the data route table to reach the server.

Example The following commands create a pool group containing 3 pools:

```
ACOS(config)# ip nat pool-group group1
ACOS(config-pool-group:group1)# member pool1
ACOS(config-pool-group:group1)# member pool2
ACOS(config-pool-group:group1)# member pool3
```

ip nat range-list

Description Configure a range of IP addresses to use with static NAT.

Syntax

```
[no] ip nat range-list list-name
local-ipaddr /mask-length
global-ipaddr /mask-length
count number
[list acl-label]
[vrid num]
```

Parameter	Description
list-name	Name of the static NAT address range.
local-ipaddr **/***mask-length*	Beginning (lowest) IP address in the range of local addresses.
global-ipaddr **/***mask-length*	Beginning (lowest) IP address in the range of global addresses.
count *number*	Number of addresses to be translated, 1-200000. The range contains a contiguous block of the number of addresses you specify. The block of local addresses starts with the address you specify for local-ipaddr. Likewise, the block of global addresses begins with the address you specify for global-ipaddr.
list *acl-label*	Specifies an ACL that matches on the range-list addresses to be translated. Valid options for acl-label include: • 0-199 —Specifies a numbered ACL. • **name** acl-name – Specifies a named ACL.
vrid *num*	VRRP-A VRID.

Default None.

Mode Configuration mode

Usage You can configure up to 2000 ranges. You can specify IPv4 or IPv6 addresses within a range.

Example The following command configures an IP address range named “nat-list-1” that maps up to 100 local addresses starting from 10.10.10.97 to Internet addresses starting from 192.168.22.50:

```
ACOS(config)# ip nat range-list nat-list-1 10.10.10.97 /16
192.168.22.50 /16 count 100
```

Related Commands:

- access-list (standard)
- access-list (extended)

ip nat template logging

Description Configure a template for external logging of SLB traffic events.

Syntax

```
[no] ip nat template logging template-name
```

This command changes the CLI to the configuration level for the specified NAT logging template, where the following commands are available.

Command	Description
[no] **facility** *facility-name*	Specifies the logging facility to use. For a list of available facilities, enter the following command: **facility ?** The default facility is local0.
[no] **include-destination**	Includes the destination IP addresses and protocol ports in NAT port mapping logs.
[no] **include-rip-rport**	Includes the IP and port of real server in logs (SLB function only).
[no] **log port-**	Enables logging for NAT mapping. • **creation**—Log only the creation of NAT

Command	Description
mappings {**creation** | **disable**}	mappings. By default, both NAT mapping creation and deletion are logged. • **disable**–Disable the logging of NAT mappings. **NOTE:** The "no" form of the command returns the logging method to its default, Syslog.
[no] **service-group** *group-name*	Specifies the service group for the external log servers.
[no] **severity** *severity-level*	Specifies the severity level to assign to LSN traffic logs generated using this template. Use the **severity ?** command to view the available severity levels. You can enter the name or the number of a severity level. The default severity is 7 (debugging).
[no] **source-port** {*source-port* | **any**}	Specifies the source protocol port the ACOS device uses to send out log messages to the external log servers (1-65535). **NOTE:** This does not conflict with the real server port, which is the destination port of the logging packet. If the **any** option is configured, the ACOS device randomly selects a source-port for each logging packet. The default source port is 514 (for UDP only).

NOTE: The source-port command is only applicable to syslog over UDP, and does not apply to TCP traffic. With syslog over TCP traffic, the source port is determined by ACOS through Smart NAT.

Default There is no NAT logging template by default. When you configure one, the template options have the default values as described in the table above.

Mode Configuration mode

Usage The template keeps track as to which external clients were mapped to the NAT IP and load balances multiple IP address requests. Therefore it can be used once VIPs are configured.

Example The following commands show a configuration for external logging of SLB NAT activity.

```
ACOS(config)# ip nat pool pool1 20.0.0.1 20.0.0.1 netmask /32
ACOS(config)# ip nat template logging testlog
ACOS(config-nat logging)# log port-mappings both
ACOS(config-nat logging)# log session
ACOS(config-nat logging)# include-destination
ACOS(config-nat logging)# include-rip-rport
ACOS(config-nat logging)# service-group log
ACOS(config-nat logging)# exit
ACOS(config)# slb server rs1 20.0.0.6
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server rs2 20.0.0.8
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server ls1 20.0.0.7
ACOS(config-real server)# port 514 udp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg1 udp
ACOS(config-slb svc group)# member ls1 514
ACOS(config-slb svc group-member:514)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb virtual-server vip1 10.0.0.111
ACOS(config-slb vserver)# template logging testlog
ACOS(config-slb vserver)# show log
```

```
Log Output:

Apr 15 14:27:04  Apr 15 14:27:03 ACOS NAT-TCP-C:
10.0.0.12:25235 -> 20.0.0.1:2097 RS 20.0.0.7:80#015
...
```

ip nat translation

Description Configure NAT timers.

Syntax

```
[no] ip nat translation
{icmp-timeout {age seconds | fast} |
ignore-tcp-msl |
service-timeout {tcp | udp} portnum {age seconds | fast} |
tcp-timeout seconds |
udp-timeout  seconds}
```

Parameter	Description
icmp-timeout {**age** *seconds* | **fast**}	Specifies the minimum number of seconds NATted ICMP sessions can remain idle before being terminated. You can specify 2-15000 seconds, or **fast**. The **fast** option terminates the session as soon as a response is received. The default is **fast**.
ignore-tcp-msl	Immediately reuse TCP sockets after session termination, without waiting for the Maximum Session Life (MSL) time to expire. This is disabled for by default.
service-timeout **{tcp | udp}** **portnum** {**age** *seconds* | **fast**}	Specifies the minimum number of seconds NATted sessions on a specific protocol port can remain idle before being terminated. The timeout set for an individual protocol port overrides the global TCP or UDP timeout for NATted sessions. You can specify 2-15000 seconds, or **fast**. The **fast** option terminates the session as soon as a response is received. By default, this is not set. For all service ports except

Parameter	Description
	UDP 53, the **tcp-timeout** or **udp-timeout** setting is used. For UDP port 53, the SLB MSL time is used.
tcp-timeout *seconds*	Timeout for TCP sessions that are not ended normally by a FIN or RST. You can specify 2-15000 seconds: The default is 300 seconds.
udp-timeout *seconds*	The supported values and timer behavior for UDP sessions are the same as those for **tcp-timeout** (described above). The default is 300 seconds.

Default See descriptions.

Mode Configuration mode

Usage The timeout value you specify is the minimum number of seconds the session can remain idle. It takes up to 60 seconds following expiration of the configured timeout value for the session to be removed.

If you specify 2-30 seconds, the timeout takes place very rapidly, as close to the configured timeout as possible.

If you specify 31-15000 seconds, the timeout value must be divisible by 60, and can be a minimum of 1 minute. If the timeout is set to a value in the range 31-59, the timeout value is rounded up to 60. Values in the range 61-14999 are rounded down to the nearest multiple of 60.

Example The following command changes the TCP timeout to 120 seconds:

```
ACOS(config)# ip nat translation tcp-timeout 120
```

ip nat-global reset-idle-tcp-conn

Description Enable client and server TCP Resets for NATted TCP sessions that become idle.

Syntax

```
[no] ip nat-global reset-idle-tcp-conn
```

Default Disabled.

Mode Configuration mode

ip prefix-list

Description Configure an IPv4 prefix list.

Syntax

```
[no] prefix-list list-name
[description string]
[seq sequence-num]
{deny | permit}
{any | ipaddr/mask-length}
[ge prefix-length] [le prefix-length]
```

Parameter	Description
list-name	Name of the IP prefix list. The name cannot contain blanks.
description *string*	Description of the IP prefix list.
seq *sequence-num*	Changes the sequence number of the IP prefix-list rule. The sequence number can be 1-4294967295.
deny | **permit**	Action to take for IP addresses that match the prefix list.
any | *ipaddr* **/***mask-length*	IP address and number of mask bits, from left to right, on which to match. If you omit the **ge** and **le** options (described below), the mask-length is also the subnet mask on which to match.
ge *prefix-length*	Specifies a range of prefix lengths on which to match. Any prefix length equal to or greater than the one specified will match. For example, **ge 25** will match on any of the following mask lengths: /25, /26, /27, /28, /29, /30, /31, or /32.
le *prefix-length*	Specifies a range of prefix lengths on which to match. Any prefix length less than or equal to the one specified will match. The lowest prefix length in the range is the prefix specified with the IP address. For example, **192.168.1.0/24 le 28** will match on any of the following mask lengths: /24, /25, /26, /27, or /28.

Default N/A

Mode Configuration mode

Usage You can use IP prefix lists to provide input to the OSPFv2 command area area-id filter-list.

How Matching Occurs

Matching begins with the lowest numbered IP prefix-list rule and continues until the first match is found. The action in the first matching rule is applied to the IP address. For example, if the IP prefix list contains the following two rules, rule 5 is used for IP address 192.168.1.9, even though the address also matches rule 10.

```
ip prefix-list 5 permit any
ip prefix-list 10 deny 192.168.1.0/24
```

The ge prefix-length and le prefix-length options enable you to specify a range of mask lengths on which to match. If you do not use either option, the mask-length in the address (/24 in the example above) specifies both the following:

- Number of bits to match, from left to right
- Mask length on which to match

If you use one or both of the `ge` or `le` options, the mask-length specifies only the number of bits to match. The `ge` or `le` option specifies the mask length(s) on which to match.

The following rule matches on any address whose first octet is 10 and whose mask-length is 8:

```
ip prefix-list match_on_8bit_mask_only permit 10.0.0.0/8
```

IP address 10.10.10.10/8 would match this rule but 10.10.10.10/24 would not.

The following rule uses the le option to extend the range of mask lengths that match:

```
ip prefix-list match_on_24bit_mask_or_less permit 10.0.0.0/8
le 24
```

This rule matches on any address that has 10 in the first octet, and whose mask length is 24 bits or less. IP addresses 10.10.10.10/8 and 10.10.10.10/24 would both match this rule.

The following rule permits any address from any network that has a mask 16-24 bits long.

```
ip prefix-list match_any_on_16-24bit_mask permit 0.0.0.0/0 ge
16 le 24
```

Implied Deny any Rule

The IP prefix list has an implied deny any rule at the end. This rule is not visible and cannot be changed or deleted. If an IP address does not match any of the rules in the IP prefix list, the ACOS device uses the implied deny any rule to deny the address.

Sequence Numbering

As described above, the sequence of rules in the IP prefix list can affect whether a given address matches a permit rule or a deny rule.

When you configure the first IP prefix-list rule, the ACOS device assigns sequence number 5 to the rule by default. After that, the sequence number for each new rule is incremented by 5. If you explicitly set the sequence number of a rule, subsequent rules are still sequenced in increasing increments of 5. For example, if you set the sequence number of the first rule to 7, the next rule is 12 by default.

You can explicitly set the sequence number of a rule when you configure the rule. You also can change the sequence number of a rule that is already configured.

Example

The following commands add descriptions to some IP prefix-list rule and display the results:

```
ACOS(config)# ip prefix-list aaa description Here_is_a_string_
to_describe_the_rule.
ACOS(config)# ip prefix-list ccc description And_here_is_a_
string_to_describe_this_rule.
ACOS(config)# show running-config | section ip prefix-list
ip prefix-list aaa description Here_is_a_string_to_describe_
the_rule.
```

```
ip prefix-list aaa seq 5 permit any
ip prefix-list bbb seq 10 permit 192.168.1.0/24
ip prefix-list ccc description And_here_is_a_string_to_
describe_this_rule.
ip prefix-list ccc seq 15 deny 10.10.10.0/8 le 24
```

ip reroute

Description Enter the ip reroute mode to suppress the reroute for a particular protocol.

Syntax

```
[no] ip reroute
```

Mode Configuration mode

Usage When routes are added, use of this command specifies not to trigger a route table version change update for the protocol that will be configured in ip reroute mode. See suppress-protocols for further information.

Example The following command enters ip reroute mode:

```
ACOS(config)# ip reroute
ACOS(config-reroute)#
```

suppress-protocols

Description Suppress the reroute trigger for a particular protocol.

Syntax

```
[no] suppress-protocols protocol
```

Parameter	Description
protocol	• `connected` - Physically connected • `ebgp` - External Border Gateway Protocol • `ibgp` - Internal Border Gateway Protocol • `isis` - Intermediate System to Intermediate System protocol • `ospf` - Open Shortest Path First protocol

Parameter	Description
	• `rip` - Routing Information Protocol • `static` - Static route

Mode IP reroute mode

Usage Specify the protocol for suppressing route table version change updates.

Example The following command enters ip reroute mode and then suppresses route table updates for static routes:

```
ACOS(config)# ip reroute
ACOS(config-reroute)# suppress-protocols static
ACOS(config-reroute-suppress-protocols)# end
ACOS# config
ACOS(config)# ip route 3.3.3.0 /24 4.4.4.3
```

ip route

Description Configure a static IP route.

Syntax

```
[no] ip route destination-ipaddr {subnet-mask | /mask-length}
{
next-hop-ipaddr
  [distance]
  [description string] |
lif num next-hop-ipaddr
  [distance]
  [description string] |
partition partition-name
  [vrid vrid]
  [description string]
tunnel num next-hop-ipaddr
  [distance]
  [description string]
}
```

Syntax

```
[no] ip route static bfd local-ipaddr remote-ipaddr
```

Parameter	Description
destination-ipaddr	Specifies the destination of the route. To configure a default route, specify 0.0.0.0/0.

Parameter	Description
{*subnet-mask* | /*mask-length*}	
next-hop-ipaddr	Specifies the next-hop router to use to reach the route destination. The address must be in the same subnet as the ACOS device.
distance	Distance value for the route, 1-255. Note that The distance value has no significance for management routes and will be displayed as zero.
partition *partition-name* [**vrid** *vrid*]	Forwards the traffic to the specified L3V partition as the next hop. The **vrid** option specifies the VRRP-A VRID, if applicable.
description *string*	Description of the static route.

Default There are no static routes configured by default.

Mode Configuration mode

Usage If a destination can be reached by an explicit route (a route that is not a default route), then the explicit route is used. If an explicit route is not available to reach a given destination, the default route is used (if a default route is configured).

If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command configures a default route using gateway 10.10.10.1 and the default metric:

```
ACOS(config)# ip route 0.0.0.0/0 10.10.10.1
```

ip tcp syn-cookie threshold

Description Modify the threshold for TCP handshake completion. The TCP handshake threshold is applicable when SYN cookies are active.

Syntax

```
[no] ip tcp syn-cookie threshold seconds
```

Parameter	Description
seconds	Number of seconds allowed for a TCP handshake to be completed. If the handshake is not completed within the allowed time, the ACOS device drops the session. You can specify 1-100 seconds.

Default 4 seconds

Mode Configuration mode

Usage The TCP handshake threshold is applicable only when software-based SYN cookies are active. To enable support for software-based SYN cookies, use the **syn-cookie enable** command at the virtual port level. (See the "syn-cookie" command in the *Command Line Interface Reference* for more information.)

Example The following command changes the TCP TCP handshake threshold to 15 seconds:

```
ACOS(config)# ip tcp syn-cookie threshold 15
```

ipv4-in-ipv6 frag

Description Configure IPv4-in-IPv6 fragmentation parameters.

Syntax

```
[no] ipv4-in-ipv6 frag
```

Default None

Mode Configuration mode

ipv6

Description Configure global IPv6 settings.

ipv6 access-list

Description Configure an extended IPv6 ACL.

Syntax

```
[no] ipv6 access-list name
```

This command changes the CLI to the configuration level for the ACL, where the following ACL-related commands are available.

Syntax

```
[no] [seq-num] {permit | deny}
{ipv6 | icmp | geo-location name | object-group name}

{any | host host-src-ipv6addr | net-src-ipv6addr /mask-length
| object-group name}

{any | host host-dst-ipv6addr | net-dst-ipv6addr /mask-length
| object-group name}

[fragments] [vlan vlan-id] [dscp num]

[log[transparent-session-only]]
```

Syntax

```
[no] [seq-num] {permit | deny} {tcp | udp}

{any | host host-src-ipv6addr | net-src-ipv6addr /mask-length
| object-group name}
  [eq src-port | gt src-port | lt src-port |
  range start-src-port end-src-port]

{any | host host-dst-ipv6addr | net-dst-ipv6addr /mask-length
| object-group name}
  [eq src-port | gt src-port | lt src-port |
  range start-src-port end-src-port]

[fragments] [vlan vlan-id] [dscp num]
  [established]

[log[transparent-session-only]]
```

Parameter	Description
seq-num	Sequence number of this rule in the ACL. You can use this option to resequence the rules in the ACL.
deny | **permit**	Action to take for traffic that matches the ACL: • **deny** – Drops the traffic. • **permit** – Allows the traffic.
ipv6 | **icmp** | **geo-location** name | **object-group** *name*	Type of traffic on which to match.

Parameter	Description
tcp | **udp**	
any | **host** *host-src-ipv6addr* | *net-src-ipv6addr* **/***prefix-length* | **object-group** *name*	Source IP address(es) to filter. • **any** – The ACL matches on all source IP addresses. • **host** *host-src-ipv6addr* – The ACL matches only on the specified host IPv6 address. • *net-src-ipv6addr* **/***prefix-length* – The ACL matches on any host in the specified subnet. • **object-group** *name* – The ACL matches on the object group.
eq *src-port* | **gt** *src-port* | **lt** *src-port* | **range** *start-src-port end-src-port*	For **tcp** or **udp**, the source protocol ports to filter. • **eq** *src-port* – The ACL matches on traffic from the specified source port. • **gt** *src-port* – The ACL matches on traffic from any source port with a higher number than the specified port. • **lt** *src-port* – The ACL matches on traffic from any source port with a lower number than the specified port. • **range** *start-src-port end-src-port* – The ACL matches on traffic from any source port within the specified range.
any | **host** *host-dst-ipv6addr* | *net-dst-ipv6addr* **/***mask-length*	Destination IP address(es) to filter.

Parameter	Description
| **object-group** *name*	
eq *dst-port* | **gt** *dst-port* | **lt** *dst-port* | **range** *start-dst-port end-dst-port*	For **tcp** or **udp**, the destination protocol ports to filter. • **eq** *dst-port* – The ACL matches on traffic from the specified destination port. • **gt** *dst-port* – The ACL matches on traffic from any destination port with a higher number than the specified port. • **lt** *dst-port* – The ACL matches on traffic from any destination port with a lower number than the specified port. • **range** *start-dst-port end-dst-port* – The ACL matches on traffic from any destination port within the specified range.
fragments	Matches on packets in which the More bit in the header is set (1) or has a non-zero offset.
vlan *vlan-id*	Matches on the specified VLAN. VLAN matching occurs for incoming traffic only.
dscp *num*	Matches on the 6-bit Diffserv value in the IP header, 1-63.
established	Matches on TCP packets in which the ACK or RST bit is not set. This option is useful for protecting against attacks from outside. Since a TCP connection from the outside does not have the ACK bit set (SYN only), the connection is dropped. Similarly, a connection established from the inside always has the ACK bit set. (The first packet to the network from outside is a SYN/ACK.)
log transparent-session-only]	Configures the ACOS device to generate log messages when traffic matches the ACL.

Syntax

```
[no] remark string
```

The **remark** command adds a remark to the ACL. The remark appears at the top of the ACL when you display it in the CLI. The string can be 1-63 characters. To use blank spaces in the remark, enclose the entire remark string in double quotes.

Default None

Mode Configuration mode

ipv6 address

Description Configure the global IPv6 address of the ACOS device, when the device is deployed in transparent mode (Layer 2 mode).

Syntax

```
[no] ipv6 address ipv6-addr/prefix-length [link-local]
[anycast]
```

Parameter	Description
ipv6-addr	Valid unicast IPv6 address.
prefix-length	Prefix length, up to 128.
link-local	Configures the address as the link-local IPv6 address for the interface, instead of a global address. Without this option, the address is a global address.
anycast	Configures the address as an anycast address. An anycast address can be assigned to more than one interface. A packet sent to an anycast address is routed to the “nearest” interface with that address, based on the distance in the routing protocol.

Default N/A

Mode Configuration mode

Usage This command applies only when the ACOS device is deployed in transparent mode. To assign IPv6 addresses to individual interfaces instead (gateway mode), use the ipv6 address command at the interface configuration level.

If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command configures global IPv6 address 2001:db8::1521:31ab/32:

```
ACOS(config)# ipv6 address 2001:db8::1521:31ab/32
```

ipv6 default-gateway

Description Specify the default gateway to use to reach other IPv6 networks, when the ACOS device is used in transparent mode (Layer 2 mode).

Syntax

```
[no] ipv6 default-gateway ipv6-addr
```

Replace *ipv6-addr* with the IPv6 address of the next-hop gateway.

Default N/A

Mode Configuration mode

Usage This command applies only when the ACOS device is used in transparent mode. If you instead want to use the device in gateway mode (Layer 3 mode), configure routing.

If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which to apply this command.

Example The following command configures default IPv6 gateway 2001:db8::1521:31ac:

```
ACOS(config)# ipv6 default-gateway 2001:db8::1521:31ac
```

ipv6 frag timeout

Description Configures the timeout for IPv6 packet fragments.

Syntax

```
[no] ipv6 frag timeout ms
```

Replace *ms* with the number of milliseconds (ms) the ACOS device buffers fragments for fragmented IPv6 packets. If any fragments of an IPv6 packet do not arrive within the specified time, the fragments are

discarded and the packet is not re-assembled. You can specify 4-65535 ms, in 10-ms increments.

Default 60000 ms

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

ipv6 icmpv6 disable

Description Disables ICMPv6 messages.

Syntax

```
[no] ipv6 icmpv6 disable {redirect | unreachable}
```

Parameter	Description
redirect	Disables sending of ICMPv6 Redirect messages.
unreachable	Disables sending of ICMPv6 Destination Unreachable messages.

Default Both types of ICMP messages are enabled.

Mode Configuration mode

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command disables sending of IPv6 ICMP Destination Unreachable messages:

```
ACOS(config)# ipv6 icmpv6 disable unreachable
```

ipv6 nat icmpv6 respond-to-ping

Description Enable ACOS to respond to ping requests sent to NAT addresses owned by the ACOS device.

Syntax

```
[no] ipv6 icmpv6 respond-to-ping
```

Default Disabled.

ipv6 nat inside source list

Description Inside configuration for IPv6 NAT.

Syntax

```
[no] ipv6 nat inside source list list-name pool pool-name
```

Parameter	Description
list-name	Name of the source list.
pool-name	Name of the address pool.

Default N/A

Mode Configuration mode

ipv6 nat pool

Description Configure a named set of IPv6 addresses for use by Network Address Translation (NAT).

Syntax

```
[no] ipv6 nat pool pool-name start-ipv6-addr end-ipv6-addr
netmask mask-length
[gateway ipaddr]
[ip-rr]
[port-overload]
[vrid num]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask *mask-length*	Network mask for the IP addresses in the pool, 64-128.
gateway *ipv6-addr*	Next-hop gateway address.
ip-rr	Uses pool IP addresses in round robin fashion. Without this option, IP address selection from a NAT

Parameter	Description
	pool depends on the incoming tuple and the usage of the NAT pool.
port-overload	Nat Pool Port overload. To process more than 65535 concurrent connections by supporting that a given SNAT address can continue to use the same source port as long as the remote socket is unique.
vrid *num*	VRRP-A VRID.

Default None.

Mode Configuration mode

Example The following command configures an IPv6 address pool named "ipv6pool2":

```
ACOS(config)# ipv6 nat pool ipv6pool2 abc1::1 abc1::10 netmask 96
```

NOTE: The IPv6 nat pool cannot be configured if the IPv6 address is used on another partition.

ipv6 nat pool-group

Description Configure a set of IPv6 pools for use by NAT. Pool groups enable you to use non-contiguous IP address ranges, by combining multiple IPv6 address pools.

Syntax

```
[no] ipv6 nat pool-group pool-group-name
[vrid num]
```

Parameter	Description
pool-group-name	Name of the pool group.
vrid *num*	VRRP-A VRID.

This command changes the CLI to the configuration level for the specified pool group, where the following command is available:

member *pool-name*

Replace *pool-name* with the name of a configured IP address pool.

Default None.

Mode Configuration mode

Usage To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

For SLB, a pool group can contain up to 5 pools. Pool group members must belong to the same protocol family (IPv4 or IPv6). A pool can be a member of multiple pool groups.

If a pool group contains pools in different subnets, the ACOS device selects the pool that matches the outbound subnet. For example, of there are two routes to a given destination, in different subnets, and the pool group has a pool for one of those subnets, ACOS selects the pool that is in the subnet for the outbound route.

The ACOS device selects the pool whose addresses are in the same subnet as the next-hop interface used by the data route table to reach the server.

ipv6 neighbor

Description Configure a static IPv6 neighbor.

Syntax

```
[no] ipv6 neighbor ipv6-addr macaddr
{ethernet port-num | trunk TrunkID | tunnel tunnel-num}
[vlan vlan-id]
```

Parameter	Description
ipv6-addr	IPv6 unicast address of the neighbor.
macaddr	MAC address of the IPv6 neighbor.
ethernet	Ethernet interface connected to the neighbor.

Parameter	Description
port-num	
trunk *trunkID*	Trunk interface connected to the neighbor.
tunnel *tunnel-num*	Tunnel interface connected to the neighbor. You can specify 1-128.
vlan-id	VLAN for which to add the IPv6 neighbor entry. If you do not specify the VLAN, the entry is added for all VLANs.

Default N/A

Mode Configuration mode

Usage The neighbor must be directly connected to the ACOS device's Ethernet port you specify, or connected through a Layer 2 switch.

If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command configures IPv6 neighbor 2001:db8::1111:2222 with MAC address abab.cdcd.efef, connected to the ACOS device's Ethernet port 5:

```
ACOS(config)# ipv6 neighbor 2001:db8::1111:2222 abab.cdcd.efef
ethernet 5
```

ipv6 ospf display route single-line

Description Change how IPv6 routes are displayed in the **show ipv6 ospf route** output.

Syntax

```
[no] ipv6 ospf display route single-line
```

Default By default, this option is disabled. Routes are displayed on multiple lines.

Mode Configuration mode

ipv6 prefix-list sequence-number

Description Configure an IPv6 prefix list.

Syntax

```
[no] prefix-list list-name
[description string]
[seq sequence-num]
{deny | permit}
{any | ipav6ddr/prefix-length}
[ge prefix-length] [le prefix-length]
```

Parameter	Description
list-name	Name of the IP prefix list. The name cannot contain blanks.
description *string*	Description of the IP prefix list.
seq *sequence-num*	Changes the sequence number of the IP prefix-list rule. The sequence number can be 1-4294967295.
deny | **permit**	Action to take for IP addresses that match the prefix list.
any | *ipav6ddr /prefix-length*	IP address and number of mask bits, from left to right, on which to match. If you omit the **ge** and **le** options (described below), the mask-length is also the subnet mask on which to match.
ge *prefix-length*	Specifies a range of prefix lengths on which to match. Any prefix length equal to or greater than the one specified will match. For example, **ge 25** will match on any of the following mask lengths: /25, /26, /27, /28, /29, /30, /31, or /32.
le *prefix-length*	Specifies a range of prefix lengths on which to match. Any prefix length less than or equal to the one specified will match. The lowest prefix length in the range is the prefix specified with the IP address. For example, **192.168.1.0/24 le 28** will match on any of the following mask lengths: /24, /25, /26, /27, or /28.

Default N/A

Mode Configuration mode

Usage You can use IP prefix lists to provide input to the OSPFv2 command area area-id filter-list.

The rules for matching and sequence numbering are the same as those for IPv4 prefix lists. (See ip prefix-list.)

iv6p reroute

Description Enter the ipv6 reroute mode to suppress the reroute for a particular protocol.

Syntax

```
[no] ipv6 reroute
```

Mode Configuration mode

Usage When routes are added, use of this command specifies not to trigger a route table version change update for the protocol that will be configured in ip reroute mode.

Example The following command enters ip reroute mode:

```
ACOS(config)# ipv6 reroute
```

Related Commands:

- suppress-protocols

suppress-protocols

Description Suppress the reroute trigger for a particular protocol.

Syntax

```
[no] suppress-protocols protocol
```

Parameter	Description
protocol	• `connected` - Physically connected • `ebgp` - External Border Gateway Protocol • `ibgp` - Internal Border Gateway Protocol • `isis` - Intermediate System to Intermediate System protocol

Parameter	Description
	• `ospf` - Open Shortest Path First protocol • `rip` - Routing Information Protocol • `static` - Static route

Mode IP reroute mode

Usage Specify the protocol for suppressing route table version change updates.

Example The following command enters ipv6 reroute mode and then suppresses route table updates for static routes:

```
ACOS(config)# ipv6 reroute
ACOS(config-reroute)# suppress-protocols static
ACOS(config-reroute-suppress-protocols)# end
ACOS# config
ACOS(config)# ip route 3.3.3.0 /24 4.4.4.3
```

ipv6 route

Description Configure a static IPv6 route.

Syntax

```
[no] ipv6 route ipv6addr/prefix-length next-hop-ipv6addr
  [ethernet num | trunk num | ve num]
  [distance]
  [description string] |

[no] ipv6 route static bfd [ethernet num | trunk num | ve num]
ipv6addr next-hop-ipv6addr
```

Parameter	Description
ipv6addr	IPv6 unicast address of the route destination.
prefix-length	Prefix length, 1-128.
next-hop-ipv6addr	IPv6 unicast address of the next-hop gateway to the destination.
distance	Distance value for the route, 1-255.

Parameter	Description
string	Description of the static route.

Default N/A

Mode Configuration mode

Usage The **ethernet**, **trunk**, and **ve** options are available only if the *ipv6addr* is a link-local address. Otherwise, the options are not displayed in the online help and are not supported.

- If you use an individual Ethernet port, the port cannot be a member of a trunk or a VE. If you use a trunk, the trunk cannot be a member of a VE.
- After you configure the static route, you cannot change the interface's membership in trunks or VEs. For example, if you configure a static route that uses Ethernet port 6's link-local address as the next hop, it is not supported to later add the interface to a trunk or VE. The static route must be removed first.

If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following command configures a static IPv6 route to destination 2001:db8::3333:3333/32, though gateway 2001:db8::3333:4444:

```
ACOS(config)# ipv6 route 2001:db8::3333:3333/32
2001:db8::3333:4444
```

Example The following command configures a default IPv6 route:

```
ACOS(config)# ipv6 route ::/0 abc1::1111
```

Example The following command configures an IPv6 static route that uses Ethernet port 6's link-local address as the next hop:

```
ACOS(config)# ipv6 route abaa:3::0/64 fe80::2 ethernet 6
```

ipv6-in-ipv4 frag

Description Configure IPv6-in-IPv4 fragmentation parameters.

Syntax `[no] ipv6-in-ipv4 frag`

Default None

Mode Configuration mode

router

Description Enter the configuration mode for a dynamic routing protocol.

Syntax `[no] router protocol`

Replace *protocol* with one of the following:

Command	Description
bgp *AS-num*	Specifies an Autonomous System (AS) for which to run Border Gateway Protocol (BGP) on the ACOS device. This also enters BGP configuration mode.
ipv6 {**ospf** [*tag*] | **rip**}	Specifies an IPv6 OSPFv3 process (1-65535) or Routing Information Protocol (RIP) process to run on the IPv6 link, and also enter configuration mode for the specified protocol.
isis [*tag*]	Enter configuration mode for Intermediate System to Intermediate System (IS-IS).
ospf [*process-id*]	Specifies an IPv4 OSPFv2 process (1-65535) to run on the ACOS device, and also enter OSPF configuration mode.
rip	Enter configuration mode for Routing Information Protocol (RIP).

Default Dynamic routing protocols are disabled by default.

Mode Configuration mode

Usage This command is valid only when the ACOS device is configured for gateway mode (Layer 3).

Example The following command enters the configuration level for OSPFv2 process 1:

```
ACOS(config)# router ospf 1
ACOS(config-ospf:1)#
```

router rip

The following is the minimum required configuration. Additional configuration may be required depending on your deployment.

- Use the **router rip** global configuration command to enable RIP and access the configuration level for global IPv4 RIP parameters:

```
ACOS(config)# router rip
ACOS(config-rip)#
```

- Use the **network** command to enable individual networks or interfaces. For example:

```
ACOS(config-rip)# network 192.168.10.10/24
ACOS(config-rip)# network ethernet 3
```

cisco-metric-behavior

Description Enable Cisco-compatible metric behavior. This option affects the display of metric values in the RIP routing table.

Syntax

```
[no] cisco-metric-behavior {enable | disable}
```

Parameter	Description
enable	The metric values displayed for routes in the RIP routing table are the values before modification by this RIP router (the ACOS device).
disable	The metric values displayed for routes in the RIP routing table are the values after modification by this RIP router (the ACOS device).

Default disable

Mode IPv4 RIP

default information originate

Description Enable generation of a default route into RIP.

Syntax

```
[no] default information originate
```

Default Disabled

Mode IPv4 RIP

default-metric

Description Configure the default metric value for routes that are redistributed into IPv4 RIP.

Syntax

```
[no] default-metric num
```

Replace *num* with the default metric, 1-16.

Default 1

Mode IPv4 RIP

distance

Description Set the administrative distance for IPv4 RIP routes.

Syntax

```
[no] distance num [ipaddr/mask-length [acl-id]]
```

Parameter	Description
num	Administrative distance, 1-255.
ipaddr /mask-length	Network prefix and mask length. The specified distance is applied only to routes with a matching source address.
acl-id	ACL ID. The specified distance is applied only to routes that match the source IP address in the ACL.

NOTE: In the ACL, use the permit action, not the deny action.

Default The default distance is 120.

Mode IPv4 RIP

Usage The administrative distance specifies the trustworthiness of routes. In cases where there are multiple routes to the same destination, from different routing protocols, the administrative distance can be used as a tie-breaker.

A low administrative distance value indicates a high level of trust. Likewise, a high administrative distance value indicates a low level of trust. For example, setting the administrative distance value for external routes to 255 means those routes are very untrustworthy and should not be used.

distribute-list

Description Configure filtering of route updates.

Syntax

```
[no] distribute-list {acl-id | prefix list-name} {in | out}
[interface]
```

Parameter	Description
acl-id | **prefix** *list-name*	ACL or prefix list that specifies the routes to filter. The action you use in the ACL or prefix list determines whether matching routes are allowed: permit – Matching routes are allowed. deny – Matching routes are prohibited.
in | **out**	Traffic direction for which to filter updates: in – Inbound route updates are filtered. out – Outbound route updates are filtered.
interface	Interface on which updates are filtered. You can specify the following types of interfaces: • `ethernet portnum` – Ethernet data interface. • `loopback [num]` – Loopback interface. If you do

Parameter	Description
	not specify an interface number, route updates are filtered out on all loopback interfaces. • `trunk trunknum` – Trunk interface. • `ve ve-num` – Virtual Ethernet (VE) interface. If no interface is specified, the filter applies to all interfaces.

NOTE: The internal option is not applicable.

Default Route updates are not filtered out.

Mode IPv4 RIP

Usage Distribute lists can be global or interface-specified:

- If you do not specify an interface with the distribute list, the list is global.
- If you do specify an interface with the distribute list, the list applies only to routes received (in) or advertised (out) on that interface.

The ACOS device can have one global inbound distribute list and one global outbound distribute list. Likewise, each interface can have one inbound distribute list and one outbound distribute list.

For inbound updates, if the interface on which the update is received has a distribute list, that distribute list is checked before the global distribute list. Likewise, for outbound updates, the distribute list on the outbound interface is checked before the global distribute list. The action (permit or deny) in the first distribute list that matches is used.

ACL Implicit Deny Rule

Every ACL has an implicit “deny any” rule at the end. Traffic that does not match any of the explicitly configured rules in an ACL will match the implicit deny rule.

Example The following commands allow incoming RIP routes only for network 30.30.30.0/24, and only when received through Ethernet interface 4:

```
ACOS(config)#ip prefix-list rip-subnet-only permit
30.30.30.0/24
ACOS(config)#router rip
ACOS(config-router)#distribute-list prefix rip-subnet-only in
ethernet 4
```

Example The following commands allow advertisement of RIP routes only for network 10.0.0.0/8, and only when advertised through VE interface 45:

```
ACOS(config)# access-list 23 permit 10.0.0.0 0.255.255.255
ACOS(config)# router rip
ACOS(config-rip)# distribute-list 23 out ve 45
```

key

Description Configure a key chain for use by RIP or IS-IS MD5 authentication.

Syntax

```
[no] key chain name
```

Replace *name* with the name of the key chain (1-31 characters).

This command changes the CLI to the configuration level for the specified key chain, where the following key-chain related command is available:

```
[no] key num
```

This command adds a key and enters configuration mode for the key. The key number can be 1-255. This command changes the CLI to the configuration level for the specified key, where the following key-related command is available:

```
[no] key-string string
```

This command configures the authentication string of the key, 1-16 characters.

Default By default, no key chains are configured.

Mode Global Config

Usage Although you can configure multiple key chains, it is recommends using one key chain per interface, per routing protocol.

Example The following commands configure a key chain named “example_chain”.

```
ACOS(config)# key chain example_chain
ACOS(config-keychain)# key 1
ACOS(config-keychain-key)# key-string thisiskey1
ACOS(config-keychain-key)# exit
ACOS(config-keychain)# key 2
ACOS(config-keychain-key)# key-string thisiskey2
ACOS(config-keychain-key)# exit
ACOS(config-keychain)# key 3
ACOS(config-keychain-key)# key-string thisiskey3
```

maximum-prefix

Description Specify the maximum number of routes allowed in the IPv4 RIP route table.

Syntax

```
[no] maximum-prefix num [threshold]
```

Parameter	Description
num	Maximum number of RIP routes allowed. You can specify 1-2048.
threshold	Percentage of the maximum number of routes at which a warning is generated. You can specify 1-100. The warnings appear in the routing log.

Default 256. The default threshold is 75 percent.

Mode IPv4 RIP

neighbor

Description Specify a neighboring IPv4 RIP router.

Syntax

```
[no] neighbor ipaddr
```

Replace *ipaddr* with the IP address of the neighboring IPv4 RIP router.

Default None

Mode IPv4 RIP

Usage Enter the command separately for each IPv4 RIP neighbor.

network

Description Enable IPv4 RIP on a network.

Syntax

```
[no] network {ipaddr/mask-length | interface}
```

Parameter	Description
ipaddr/mask-length	Prefix and mask length of a IPv4 RIP network.
interface	Interface on which to enable RIP. You can specify the following types of interfaces: • `ethernet portnum` – Ethernet data interface. • `loopback [num]` – Loopback interface. If you do not specify an interface number, RIP is enabled on all loopback interfaces. • `trunk trunknum` – Trunk interface. • `ve ve-num` – Virtual Ethernet (VE) interface. If no interface is specified, RIP is enabled on all the interfaces.

Default None

Mode IPv4 RIP

offset-list

Description Increase the metric for specific routes.

Syntax

```
[no] offset-list acl-id {in | out} offset [interface]
```

Parameter	Description
acl-id	ACL that matches on the routes for which to increase the metric.
in | out	Direction to which to apply the metric: • `in` – Applies the additional metric value to routes received in updates from RIP neighbors. • `out` – Applies the additional metric value to routes advertised to RIP neighbors.
offset	Additional metric to add to routes. You can specify 0-16.
interface	Interface on which to increase the metric. You can specify the following types of interfaces: • `ethernet portnum` – Ethernet data interface. • `loopback [num]` – Loopback interface. If you do not specify an interface number, the metric is increased on all loopback interfaces. • `trunk trunknum` – Trunk interface. • `ve ve-num` – Virtual Ethernet (VE) interface. If no interface is specified, the metric is increased on all interfaces.

Default Not set. The metric that is otherwise applied to the route by the RIP process is used.

Mode IPv4 RIP

passive-interface

Description Block RIP broadcasts from being sent on an interface.

Syntax `[no] passive-interface interface`

Replace interface with the interface on which to block RIP broadcasts. You can specify the following types of interfaces:

- `ethernet portnum` – Ethernet data interface.
- `loopback [num]` – Loopback interface. If you do not specify an interface number, RIP broadcasts are blocked on all loopback interfaces.
- `trunk trunknum` – Trunk interface.
- `ve ve-num` – Virtual Ethernet (VE) interface.

Default None. RIP broadcasts are not blocked on any interfaces.

Mode IPv4 RIP

recv-buffer-size

Description Configure the receive buffer size for RIP UDP packets.

Syntax

```
[no] recv-buffer-size bytes
```

Replace *bytes* with the maximum RIP UDP packet size allowed. You can specify 8192-2147483647 bytes.

Default 8192

Mode IPv4 RIP

redistribute

Description Redistribute route information from other sources into RIP.

Syntax

```
[no] redistribute
{
bgp [options] |
connected [options] |
floating-ip [options] |
ip-nat-list [options] |
ip-nat [options] |
isis [options] |
lw4o6 [options] |
ospf [options] |
static [options] |
vip [only-flagged | only-not-flagged [options]]
}
```

Parameter	Description
bgp *[options]*	Redistributes route information from Border Gateway Protocol (BGP) into RIP.
connected *[options]*	Redistributes route information for directly connected networks into RIP.
floating-ip *[options]*	Redistributes route information for floating IP addresses into RIP.
ip-nat-list *[options]*	Redistributes routes into RIP for reaching translated NAT addresses allocated from a range list.
ip-nat *[options]*	Redistributes routes into RIP for reaching translated NAT addresses allocated from a pool.
isis *[options]*	Redistributes route information from Intermediate System to Intermediate System (IS-IS) into RIP.
lw406 *[options]*	Redistributes routes into OSPF for Lightweight 4over6. (This is an IPv6 Migration feature.)
ospf *[options]*	Redistributes route information from Open Shortest Path First (OSPF) into RIP.
static *[options]*	Redistributes routes into RIP for reaching networks through static routes.
vip [**only-flagged** | **only-not-flagged** *[options]*]	Redistributes routes into RIP for reaching virtual server IP addresses. To control which VIPs are redistributed, use one of the following options: • **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used. • **only-not-flagged** – Redistributes all VIPs except those on which the **redistribution-flagged** command is used. • *options* - Optional parameters supported for the options listed above:

Parameter	Description
	• **metric** *num* – Metric for the route, 0-16. There is no default. • **route-map** *map-name* – Name of a route-map.

Default Disabled. By default, RIP routes are not redistributed. For other defaults, see above.

Mode IPv4 RIP

Usage When you enable redistribution, routes to all addresses of the specified type are redistributed. The **vip** option can be used to control which routes to VIPs are redistributed into RIP.

VIP Redistribution

You can exclude redistribution of individual VIPs using one or the other of the following methods.

- If more VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to allow to be redistributed, enter the following command: **redistribution-flagged**
  - At the configuration level for the RIP process, enter the following command: **redistribute vip only-flagged**
- If fewer VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to exclude from redistribution, enter the following command: **redistribution-flagged**
  - At the configuration level for the RIP process, enter either of the following commands: **redistribute vip only-not-flagged** or **redistribute vip**

NOTE: In the configuration, the **redistribute vip** command is automatically converted into the **redistribute vip only-not-flagged** command. When you display the configuration, it will contain the **redistribute vip only-not-flagged** command, not the **redistribute vip** command.

VIP Redistribution Usage Examples:

- If you have 10 VIPs and all of them need to be redistributed by RIP, use the **redistribute vip** command at the configuration level for the RIP process.
- If you have 10 VIPs but only 2 of them need to be redistributed, use the **redistribution-flagged** command at the configuration level for each of the 2 VIPs, then use the **redistribute vip only-flagged** command at the configuration level for the RIP process.
- If you have 10 VIPs and need to redistribute 8 of them, use the **redistribution-flagged** command at the configuration level for the 2 VIPs that should not be redistributed. Enter the **redistribute vip only-not-flagged** command at the configuration level for the RIP process. (In this case, alternatively, you could enter **redistribute vip** instead of **redistribute vip only-not-flagged**.)

Example The following commands redistribute floating IP addresses and VIP addresses into RIP:

```
ACOS(config-router)# redistribute floating-ip
ACOS(config-router)# redistribute vip
```

Example The following commands flag a VIP, then configure RIP to redistribute only that flagged VIP. The other (unflagged) VIPs will not be redistributed.

```
ACOS(config)# slb virtual-server vip1
ACOS(config-slb vserver)# redistribution-flagged
ACOS(config-slb vserver)# exit
ACOS(config)# router rip
ACOS(config-rip)# redistribute vip only-flagged
```

route

Description Configure static RIP routes.

Syntax `[no] route ipaddr/prefix-length`

Replace *ipaddr/prefix-length* with the destination of the route.

Default None

Mode IPv4 RIP

timers

Description Configure RIP timers.

Syntax `[no] timers basic update timeout garbage-collection`

Parameter	Description
update	Amount of time between transmission of RIP route updates to neighbors. You can specify 5-2147483647 seconds. The default is 30 seconds.
timeout	Maximum number of seconds the ACOS device waits for an update to a RIP route before the route becomes invalid. You can specify 5-2147483647 seconds. An invalid route remains in the route table and is not actually removed until the garbage-collection timer expires. (See below.) The default is 180 seconds.
garbage-collection	Amount of time after a route becomes invalid that the route remains in the route table before being removed. You can specify 5-2147483647 seconds. The default is 120 seconds.

Default See descriptions.

Mode IPv4 RIP

Usage All RIP routers in the network should use the same timer values. However, the timers should not be synchronized among multiple routers, since this can cause unnecessary collisions.

version

Description Specify the RIP version to run.

Syntax

```
[no] version {1 [2] | 2}
```

Parameter	Description
1	RIP version 1.
2	RIP version 2.

Default 2

Mode IPv4 RIP

Usage The version you specify runs on all RIP interfaces on the ACOS device.

RIPv1 is less secure than RIPv2. It is recommended to run RIPv2 if your other routers support it.

router ipv6 rip

The following is the minimum required configuration. Additional configuration may be required depending on your deployment.

- Use the **router ipv6 rip** global configuration command to enable RIP and access the configuration level for global IPv4 RIP parameters:

```
ACOS(config)# router ipv6 rip
ACOS(config-rip)#
```

- To enable IPv6 RIP on an individual interface, access the interface. For example:

```
ACOS(config)# interface ethernet 6
ACOS(config-if:ethernet:6)#
ACOS(config-if:ethernet:6)# ipv6 router rip
```

aggregate-address

Description Configure an aggregate of multiple IPv6 RIP routes.

Syntax

```
[no] aggregate-address ipv6addr/mask-length
```

Replace *ipv6addr/mask-length* with the IPv6 address and prefix length of the aggregate. The aggregate route will be used instead of the individual routes to destinations that match the aggregate's address and prefix.

Default None

Mode IPv6 RIP

cisco-metric-behavior

Description Enable Cisco-compatible metric behavior. This option affects the display of metric values in the RIP routing table.

Syntax

```
[no] cisco-metric-behavior {enable | disable}
```

Parameter	Description
enable	The metric values displayed for routes in the RIP routing table are the values before modification by this RIP router (the ACOS device).
disable	The metric values displayed for routes in the RIP routing table are the values after modification by this RIP router (the ACOS device).

Default disable

Mode IPv6 RIP

default-information originate

Description Enable generation of a default route into RIP.

Syntax

```
[no] default-information originate
```

Default Disabled

Mode IPv6 RIP

default-metric

Description Configure the default metric value for routes that are redistributed into IPv6 RIP.

Syntax

```
[no] default-metric num
```

Replace *num* with the default metric, 1-16.

Default 1

Mode IPv6 RIP

distribute-list

Description Configure filtering of route updates.

Syntax

```
[no] distribute-list {acl-id | prefix list-name} {in | out}
[interface]
```

Parameter	Description
acl-id | **prefix** *list-name*	ACL or prefix list that specifies the routes to filter. The action you use in the ACL or prefix list determines whether matching routes are allowed: • **permit** – Matching routes are allowed. • **deny** – Matching routes are prohibited.
in | **out**	Traffic direction for which to filter updates: • **in** – Inbound route updates are filtered. • **out** – Outbound route updates are filtered.
interface	Interface on which updates are filtered. You can specify the following types of interfaces: • **ethernet** *portnum* – Ethernet data interface. • **loopback** [*num*] – Loopback interface. If you do not specify an interface number, route updates

Parameter	Description
	are filtered out on all loopback interfaces. • **trunk** *trunknum* – Trunk interface. • **ve** *ve-num* – Virtual Ethernet (VE) interface. If no interface is specified, the filter applies to all interfaces.

Default Route updates are not filtered out.

Mode IPv6 RIP

Usage Distribute lists can be global or interface-specified:

- If you do not specify an interface with the distribute list, the list is global.
- If you do specify an interface with the distribute list, the list applies only to routes received (in) or advertised (out) on that interface.

The ACOS device can have one global inbound distribute list and one global outbound distribute list. Likewise, each interface can have one inbound distribute list and one outbound distribute list.

For inbound updates, if the interface on which the update is received has a distribute list, that distribute list is checked before the global distribute list. Likewise, for outbound updates, the distribute list on the outbound interface is checked before the global distribute list. The action (permit or deny) in the first distribute list that matches is used.

ACL Implicit Deny Rule

Every ACL has an implicit “deny any” rule at the end. Traffic that does not match any of the explicitly configured rules in an ACL will match the implicit deny rule.

neighbor

Description Specify a neighboring IPv6 RIP router.

Syntax

```
[no] neighbor ipv6addr interface
```

Parameter	Description
ipv6addr	Link-local IPv6 address of the neighboring IPv6 RIP router.
interface	Interface on which the neighbor can be reached. You can specify the following types of interfaces:

Default None

Mode IPv6 RIP

Usage Enter the command separately for each IPv4 RIP neighbor.

offset-list

Description Increase the metric for specific routes.

Syntax `[no] offset-list acl-id {in | out} offset [interface]`

Parameter	Description
acl-id	ACL that matches on the routes for which to increase the metric.
in | **out**	Direction to which to apply the metric: • `in`– Applies the additional metric value to routes received in updates from RIP neighbors. • `out` – Applies the additional metric value to routes advertised to RIP neighbors.
offset	Additional metric to add to routes. You can specify 0-16.
interface	Interface on which to increase the metric. You can specify the following types of interfaces: • `ethernet portnum` – Ethernet data interface. • `loopback [num]` – Loopback interface. If you do not specify an interface number, the metric is increased on all loopback interfaces.

Parameter	Description
	• `trunk trunknum` – Trunk interface. • `ve ve-num` – Virtual Ethernet (VE) interface. If no interface is specified, the metric is increased on all interfaces.

Default Not set. The metric that is otherwise applied to the route by the RIP process is used.

Mode IPv6 RIP

passive-interface

Description Block RIP broadcasts from being sent on an interface.

Syntax

```
[no] passive-interface interface
```

Replace *interface* with the interface on which to block RIP broadcasts. You can specify the following types of interfaces:

- `ethernet portnum` – Ethernet data interface.
- `loopback [num]` – Loopback interface. If you do not specify an interface number, RIP broadcasts are blocked on all loopback interfaces.
- `trunk trunknum` – Trunk interface.
- `ve ve-num` – Virtual Ethernet (VE) interface.

Default None. RIP broadcasts are not blocked on any interfaces.

Mode IPv6 RIP

recv-buffer-size

Description Configure the receive buffer size for RIP UDP packets.

Syntax

```
[no] recv-buffer-size bytes
```

Replace *bytes* with the maximum RIP UDP packet size allowed. You can specify 8192-2147483647 bytes.

Default 8192

Mode IPv6 RIP

redistribute

Description Redistribute route information from other sources into RIP.

Syntax

```
[no] redistribute
{
bgp [options] |
connected [options] |
floating-ip [options] |
ip-nat [options] |
ip-nat-list [options] |
isis [options] |
ospf [options] |
static [options] |
vip [only-flagged | only-not-flagged [options]]
}
```

Parameter	Description
bgp *[options]*	Redistributes route information from Border Gateway Protocol (BGP) into RIP.
connected *[options]*	Redistributes route information for directly connected networks into RIP.
floating-ip *[options]*	Redistributes route information for floating IP addresses into RIP.
ip-nat *[options]*	Redistributes routes into RIP for reaching translated NAT addresses allocated from a pool.
ip-nat-list *[options]*	Redistributes routes into RIP for reaching translated NAT addresses allocated from a range list.
isis *[options]*	Redistributes route information from Intermediate System to Intermediate System (IS-IS) into RIP.
ospf *[options]*	Redistributes route information from Open Shortest Path First (OSPF) into RIP.
static *[options]*	Redistributes routes into RIP for reaching networks through static routes.
vip	Redistributes routes into RIP for reaching virtual

Parameter	Description
[**only-flagged** | **only-not-flagged** | [*options*]]	server IP addresses. To control which VIPs are redistributed, use one of the following options: • **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used. • **only-not-flagged** – Redistributes all VIPs except those on which the **redistribution-flagged** command is used. • *options* - Optional parameters supported for the options listed above: • **metric** *num* – Metric for the route, 0-16. There is no default. • **route-map** *map-name* – Name of a route-map.

Default Disabled. By default, RIP routes are not redistributed. For other defaults, see above.

Mode IPv6 RIP

Usage When you enable redistribution, routes to all addresses of the specified type are redistributed. The **vip** option can be used to control which routes to VIPs are redistributed into RIP.

VIP Redistribution

You can exclude redistribution of individual VIPs using one or the other of the following methods.

- If more VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to allow to be redistributed, enter the following command: **redistribution-flagged**
  - At the configuration level for the RIP process, enter the following command: **redistribute vip only-flagged**

- If fewer VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to exclude from redistribution, enter the following command: **`redistribution-flagged`**
  - At the configuration level for the RIP process, enter either of the following commands: **`redistribute vip only-not-flagged`** or **`redistribute vip`**

NOTE: In the configuration, the **`redistribute vip`** command is automatically converted into the **`redistribute vip only-not-flagged`** command. When you display the configuration, it will contain the **`redistribute vip only-not-flagged`** command, not the **`redistribute vip`** command.

VIP Redistribution Usage Examples:

- If you have 10 VIPs and all of them need to be redistributed by RIP, use the **`redistribute vip`** command at the configuration level for the RIP process.
- If you have 10 VIPs but only 2 of them need to be redistributed, use the **`redistribution-flagged`** command at the configuration level for each of the 2 VIPs, then use the **`redistribute vip only-flagged`** command at the configuration level for the RIP process.
- If you have 10 VIPs and need to redistribute 8 of them, use the **`redistribution-flagged`** command at the configuration level for the 2 VIPs that should not be redistributed. Enter the **`redistribute vip only-not-flagged`** command at the configuration level for the RIP process. (In this case, alternatively, you could enter **`redistribute vip`** instead of **`redistribute vip only-not-flagged`**.)

route

Description Configure static RIP routes.

Syntax **`[no] route`** *`ipv6addr/prefix-length`*

Replace *`ipv6addr/prefix-length`* with the destination of the route.

Default None

Mode IPv6 RIP

route-map

Description Configure a list of interfaces to use as input to other RIP commands.

Syntax

```
[no] route-map map-name {in | out} interface
```

Parameter	Description
map-name	Name of the route map.
in | **out**	Direction to which the map applies: • `in` – Applies to incoming routes received in updates from RIP neighbors. • `out` – Applies to routes advertised to RIP neighbors.
interface	Interface to which to apply the route map. You can specify the following types of interfaces: • `ethernet portnum` – Ethernet data interface. • `loopback [num]` – Loopback interface. If you do not specify an interface number, the route map is applied to all loopback interfaces. • `trunk trunknum` – Trunk interface. • `ve ve-num` – Virtual Ethernet (VE) interface.

Default None

Mode IPv6 RIP

timers

Description Configure RIP timers.

Syntax

```
[no] timers basic update timeout garbage-collection
```

Parameter	Description
update	Amount of time between transmission of RIP route updates to neighbors. You can specify 5-2147483647 seconds. The default is 30 seconds.
timeout	Maximum number of seconds the ACOS device waits for an update to a RIP route before the route becomes invalid. You can specify 5-2147483647 seconds. An invalid route remains in the route table and is not actually removed until the garbage-collection timer expires. (See below.) The defaul tis 180 seconds.
garbage-collection	Amount of time after a route becomes invalid that the route remains in the route table before being removed. You can specify 5-2147483647 seconds. The default is 120 seconds.

Default See descriptions.

Mode IPv6 RIP

Usage All RIP routers in the network should use the same timer values. However, the timers should not be synchronized among multiple routers, since this can cause unnecessary collisions.

router ospf

To enable OSPFv2, use the following command:

```
ACOS(config)# router ospf [process-id]
```

The *process-id* specifies the IPv4 OSPFv2 process to run on the ACOS device, and can be 1-65535.

area area-id authentication

Description Enables authentication for an OSPF area.

Syntax `[no] area area-id authentication [message-digest]`

The **message-digest** option enables MD5 authentication. If you omit this option, simple text authentication is used.

NOTE: The **message-digest** option is not supported in FIPS mode.

Default Disabled. No authentication is used.

Mode OSPFv2

area area-id filter-list

Description Filter the summary routes advertised by this OSPF router, if it is acting as an Area Border Router (ABR).

Syntax

```
[no] area area-id filter-list
{access acl-id {in | out} | prefix list-name {in | out}}
```

Parameter	Description
area-id	Area ID, either an IP address or a number.
access *acl-id* {**in** | **out**}	ID of an Access Control List (ACL). The only routes that are advertised are routes to the subnets permitted by the ACL.
prefix *list-name* {**in** | **out**}	ID of an IP prefix list. The only routes that are advertised are routes to the subnets that match the list.

Default Not set.

Mode OSPFv2

Usage You can specify an ACL or an IP prefix list.

Related Commands:

- ipv6 access-list
- ip prefix-list

area area-id multi-area-adjacency

Description Enables support for multiple OSPF area adjacencies on the specified interface.

Syntax

```
[no] area area-id multi-area-adjacency
{ethernet portnum | loopback num | management | ve ve-num }
neighbor ipaddr
```

Default Disabled. By default, only one OSPF adjacency is allowed on an interface for a given OSPF process.

Mode OSPFv2

Usage This command is applicable only if this OSPF router is an ABR.

area area-id nssa

Description Configure a not-so-stubby area (NSSA).

Syntax

```
[no] area area-id nssa
[
default-information-originate
  [metric num] [metric-type {1 | 2}] |
no-redistribution |
no-summary |
translator-role {always | candidate | never}
]
```

Parameter	Description
area-id	Area ID.
default-information-originate [**metric** *num*] [**metric-type** {**1** | **2**}]	Generates a Type 7 LSA into the NSSA area. (This option takes effect only on Area Border Routers (ABRs)): • **metric** *num* – Metric for the default route, 0-16777214. The default is 20. • **metric-type** {**1** | **2**} – External link type associated with the route advertised into the OSPF routing domain: ◦ **1** – Type 1 external route

Parameter	Description
	◦ **2** – Type 2 external route
no-redistribution	Disables redistribution of routes into the area.
no-summary	Disables sending summary LSAs into the NSSA.
translator-role {**always** | **candidate** | **never**}	Specifies the types of LSA translation performed by this OSPF router for the NSSA: • **always** – If this OSPF router is an NSSA border router, the router will always translate Type 7 LSAs into Type 5 LSAs, regardless of the translator state of other NSSA border routers. • **candidate** – If this OSPF router is an NSSA border router, the router is eligible to be elected the Type 7 NSSA translator. • **never** – This OSPF router is ineligible to be elected the Type 7 NSSA translator.

Default None

Mode OSPFv2

Example The following command configures an NSSA with area ID 6.6.6.6:

```
ACOS(config)# router ospf
ACOS(config-ospf)# area 6.6.6.6 nssa
```

area area-id shortcut

Description Configure short-cutting through an area.

Syntax `[no] area area-id shortcut {default | disable | enable}`

Parameter	Description
area-id	Area ID.
default	Enables the default shortcut behavior. (See below.)

Parameter	Description
disable	Disables shortcutting through the area.
enable	Forces shortcutting through the area.

Default None

Mode OSPFv2

Usage A shortcut enables traffic to go through a non-backbone area with a lower metric, regardless of whether the ABR router is attached to the backbone area.

compatible rfc1583

Description Enable calculation of summary route costs per RFC 1583.

Syntax

```
[no] compatible rfc1583
```

Default Disabled. Summary route costs are calculated based on RFC 2328.

Mode OSPFv2

distance

Description Set the administrative distance for OSPF routes, based on route type.

Syntax

```
[no] distance
{ num | ospf {external | inter-area | intra-area} num }
```

Parameter	Description
num	Sets the administrative distance for all route types. You can specify 1-255.
ospf {**external** | **inter-area** | **intra-area**}	Sets the administrative distance for specific route types: • **external** – Routes that OSPF learns from other routing domains by redistribution. • **intra-area** – Routes within the same OSPF area. • **inter-area** – Routes between OSPF areas.

Parameter	Description
num	You can use the **ospf** option with one or more of its suboptions. For each route type, you can specify 1-255.

Default For all route types, the default administrative distance is 110.

Mode OSPFv2

Usage The administrative distance specifies the trustworthiness of routes. A low administrative distance value indicates a high level of trust. Likewise, a administrative distance value indicates a low level of trust. For example, setting the administrative distance value for external routes to 255 means those routes are very untrustworthy and should not be used.

distribute-list

Description Filter the networks received or sent in route updates.

Syntax

```
[no] distribute-list acl-id
{in | out { connected | floating-ip | ip-nat |
  ip-nat-list | ospf | static | vip}
```

Parameter	Description
acl-id	ID of an ACL. Only the networks permitted by the ACL will be allowed.
in	Uses the specified ACL to filter routes received by OSPF from other sources. The filter applies to routes from all sources.
out *route-type*	Uses the specified ACL to filter routes advertised by OSPF to other routing domains. The route-type can be one of the following: • connected – Filters advertisement of directly connected networks. • floating-ip – Filters advertisement of networks for floating IP addresses.

Parameter	Description
	• ip-nat – Filters advertisement of networks that are translated NAT addresses allocated from a pool. • ip-nat-list – Filters advertisement of networks that are translated NAT addresses allocated from a range list. • ospf [process-id] – Filters advertisement of networks to another OSPF process. • static [only-flagged | only-not-flagged] – Filters advertisement of networks reached by static routes. • vip [only-flagged | only-not-flagged] – Filters advertisement of networks to reach VIPs. ◦ By default, the option applies to all VIPs. To restrict the option to a subset of VIPs, use one of the following options: ◦ only-flagged – Redistributes only the VIPs on which the redistribution-flagged command is used. ◦ only-not-flagged – Redistributes all VIPs except those on which the redistribution-flagged command is used.

Default None

Mode OSPFv2

host ipaddr area

Description Configure a stub host entry for an area.

Syntax

```
[no] host ipaddr area area-id [cost num]
```

Parameter	Description
ipaddr	IP address of the host.
area *area-id*	OSPF area where the host is located.
cost *num*	Cost of the stub host entry, 0-65535.

Default None

Mode OSPFv2

Usage Routes to the host are listed in router LSAs as stub links.

log-adjacency-changes

Description Log adjacency changes.

Syntax

```
[no] log-adjacency-changes {detail | disable}
```

Parameter	Description
detail	Log changes in adjacency state.
disable	Disable logging of adjacency state changes.

Default Enabled by default.

Mode OSPFv2

Example The following example disables logging of adjacency state changes:

```
ACOS(config)# router ospf
ACOS(config-ospf)# log-adjacency-changes disable
```

maximum-area

Description Set the maximum number of OSPF areas supported for this OSPF process.

Syntax

```
[no] maximum-area num
```

Replace *num* with the maximum number of areas allowed for this OSPF process. You can specify 1-4294967294.

Default 4294967294

Mode OSPFv2

neighbor

Description Configure an OSPF neighbor that is located on a non-broadcast network.

Syntax

```
[no] neighbor ipaddr
[cost num |
poll-interval seconds [priority num] |
priority num [poll-interval seconds]
]
```

Parameter	Description
ipaddr	IP address of the OSPF neighbor.
cost *num*	Specifies the link-state metric to the neighbor, 1-65535. By default, no cost is set.
poll-interval *seconds*	Number of seconds this OSPF router will wait for a reply to a hello message sent to the neighbor, before declaring the neighbor to be offline. You can specify 1-65535 seconds. The default is 120 seconds.
priority *num*	Router priority of the neighbor, 1-255. By default, no priority is set.

Default No neighbors on non-broadcast networks are configured by default. When you configure one, the other parameters have the default settings described in the table above.

Mode OSPFv2

Usage This command is required only for neighbors on networks. Adjacencies to neighbors on other types of networks are automatically established by the OSPF protocol.

It is recommended to set the poll-interval to a much higher value than the hello interval.

network

Description Enable OSPF routing for an area, on interfaces that have IP addresses in the specified area subnet.

Syntax

```
[no] network
ipaddr {/mask-length  | wildcard-mask}
area area-id
[instance-id  num]
```

Parameter	Description
ipaddr {**/***mask-length* | *wildcard-mask*}	Subnet of the area. You can specify the subnet in CIDR format (ipaddr/mask-length) or as ipaddr wildcard-mask. In a wildcard-mask, 0s represent the network portion and 1s represent the host portion. For example, for a subnet that has 254 hosts and a 24-bit network mask, the **wildcard-mask** is 0.0.0.255.
area *area-id*	Area ID.
instance-id *num*	Range of OSPF instances for which to enable OSPF routing for the area, 0-255. If you omit this option, OSPF routing is enabled for all OSPF instances that are running on interfaces that have IP addresses in the specified area subnet.

Default None

Mode OSPFv2

Example The following command configures an OSPF network:

```
ACOS(config)# router ospf
ACOS(config-ospf)# network 10.10.20.20/24 area 10.10.20.30
```

ospf abr-type

Description Specify the Area Border Router (ABR) type.

Syntax

```
[no] ospf abr-type {cisco | ibm | shortcut | standard}
```

Parameter	Description
cisco	Alternative ABR using Cisco implementation (RFC 3509).
ibm	Alternative ABR using IBM implementation (RFC 3509).
shortcut	Shortcut ABR (draft-ietf-ospf-shortcut-abr-02.txt).
standard	Standard ABR behavior (RFC 2328)

Default **cisco**

Mode OSPFv2

ospf router-id

Description Set the value used by this OSPF router to identify itself when exchanging route information with other OSPF routers.

Syntax `[no] ospf router-id ipaddr`

Default For OSPFv2, the default router ID is the highest-numbered IP address configured on any of the ACOS device's loopback interfaces. If no loopback interfaces are configured, the highest-numbered IP address configured on any of the ACOS device's other Ethernet data interfaces is used.

NOTE: Setting the router ID is strongly recommended for OSPFv2.

Mode OSPFv2

Usage The ACOS device has only one router ID. The address does not need to match an address configured on the ACOS device. However, the address must be an IPv4 address and must be unique within the routing domain.

New or changed router IDs require a restart of the OSPF process. To restart the OSPF process, use the **clear ip ospf process** command.

Example The following commands set the router ID to 2.2.2.2 and reload OSPF to place the new router ID into effect:

```
ACOS(config)# router ospf
ACOS(config-ospf)# router-id 2.2.2.2
ACOS(config-ospf)# clear ip ospf process
```

overflow database

Description Specify the maxim number of LSAs or the maximum size of the external database.

Syntax

```
[no] overflow database
{max-lsa [hard | soft] | external max-lsa recover-time}
```

Parameter	Description
max-lsa [**hard** | **soft**]	Specifies the maximum number of LSAs per OSPF process, 0-4294967294. To configure the action to take if the LSA limit is exceeded: • **hard** – Shut down the OSPF process for the process. • **soft** – Issue a warning message without shutting down the OSPF process for the process.
external *max-lsa recover-time*	Specifies the maximum number of AS-external-LSAs the OSPF router can receive, 0-2147483647. The *recover-time* option specifies the number of seconds OSPF waits before attempting to recover after *max-lsa* is exceeded. You can specify 0-65535 seconds. To disable recovery, specify 0.

Default The default *max-lsa* is 2147483647.

Mode OSPFv2

summary-address

Description Summarize or disable advertisement of external routes for a specific IP address range. A summary-address helps reduce the size of the OSPF link-state database.

Syntax `[no] summary-address ipaddr/mask {not-advertise | tag num}`

Parameter	Description
ipaddr /mask	Specifies the address range.
not-advertise	Disables advertisement of routes for the specified range.
tag *num*	Includes the specified tag value in external LSAs for IP addresses within the specified range. The tag value can be 0-4294967295. The default tag value is 0.

Default None

Mode OSPFv2

router ipv6 ospf

To enable OSPFv3, use the following command:

```
ACOS(config)# router ipv6 ospf [tag]
```

The *tag* specifies the IPv6 OSPFv3 process to run on the IPv6 link, and can be 1-65535.

NOTE: It is recommended to set a fixed router-ID for all dynamic routing protocols you plan to use on the ACOS device, to prevent router-ID changes caused by VRRP-A failover.

NOTE: For OSPFv3, the area tag ID configured on an interface must be the same as the tag ID for the OSPF instance.

In addition to global parameters, OSPF has parameters on the individual interface level. To configure OSPF on an interface, use the **interface** command to access the configuration level for the interface, then use the **ip ospf** or **ipv6 ospf** command.

area area-id default-cost

Description Specify the cost of a default summary route sent into a stub area.

Syntax `[no] area area-id default-cost num`

Parameter	Description
area-id	Area ID, either an IP address or a number.
num	Cost of the default summary route, 0-16777214.

Default The default is 1.

Mode OSPFv2 or OSPFv3

Example The following command assigns a cost of 4400 to default summary routes injected into stub areas:

```
ACOS(config-ospf:1)#area 5.5.5.5 default-cost 4400
```

area area-id range

Description Summarize routes at an area boundary.

Syntax

```
[no] area area-id range ipaddr/mask-length
[advertise | not-advertise]
```

Parameter	Description
area *area-id*	Beginning area ID (either an IP address or a number).
range	Ending area ID.
ipaddr	Subnet address for the range.
/*mask-length*	Network mask length for the range.
advertise	Generates Type 3 summary LSAs for the areas in the range.
not-advertise	Does not generate Type 3 summary LSAs. The networks are hidden from other networks.

Default There is no default range configuration. When you configure a range, the default advertisement string is advertise.

Mode OSPFv2 or OSPFv3

Example The following command configures a range and disables advertisement of routes into the areas:

```
ACOS(config-ospf:1)#area 8.8.8.8 range 10.10.10.10/16 not-
advertise
```

area area-id stub

Description Configure a stub area.

Syntax

```
[no] area area-id stub [no-summary]
```

Parameter	Description
area-id	Area ID.
no-summary	ABRs do not send summary LSAs into the stub area.

Default None

Mode OSPFv2 or OSPFv3

Example The following command configures a stub area with area ID 10.2.4.5:

```
ACOS(config-ospf:1)#area 10.2.4.5 stub
```

area area-id virtual-link

Description Configure a link between two backbone areas that are separated by non-backbone areas.

Syntax

```
[no] area area-id virtual-link ipaddr
[authentication]
[authentication-key string [string ...]]
[dead-interval seconds]
[fall-over bfd]
[hello-interval seconds]
[message-digest-key num md5 string [string ...]]
[retransmit-interval seconds]
[transmit-delay seconds]
```

Parameter	Description
area-id	Area ID, either an IP address or a number.
ipaddr	IP address of the OSPF neighbor at the other

Parameter	Description
	end of the link.
authentication	Enables authentication on the link.
authentication-key string *[string ...]*	Specifies a simple text password for authenticating OSPF traffic between this router and the neighbor at the other end of the virtual link. The string is an 8-character authentication password.
dead-interval *seconds*	Number of seconds this OSPF router will wait for a reply to a hello message sent to the neighbor on the other end of the virtual link, before declaring the neighbor to be offline. You can specify 1-65535 seconds. The default is 40 seconds.
fall-over bfd	Enables fall-over detection.
hello-interval *seconds*	Number of seconds this OSPF router waits between sending hello messages to the neighbor on the other end of the virtual link. You can specify 1-65535 seconds. The default is 10 seconds.
message-digest-key *num* **md5** *string* *[string ...]*	Specifies an MD5 key, 1-255. The string is a 16-character authentication password. **NOTE:** The **message-digest-key** option is not supported in FIPS mode.
retransmit-interval seconds	Number of seconds this OSPF router waits before resending an unacknowledged packet to the neighbor on the other end of the virtual link. You can specify 1-65535 seconds. The default is 5 seconds.
transmit-delay	Number of seconds this OSPF router waits

Parameter	Description
seconds	between sending packets to the neighbor on the other end of the virtual link. You can specify 1-65535 seconds. The default is 1 second.

Default None. When you configure a virtual link, it has the default settings described in the table above.

Mode OSPFv2 or OSPFv3

auto-cost reference bandwidth

Description Change the reference bandwidth used by OSPF to calculate default metrics.

Syntax

```
[no] auto-cost reference-bandwidth mbps
```

Replace *mbps* with the reference bandwidth, in Mbps. You can specify 1-4294967.

Default 10000 Mbps

Mode OSPFv2 or OSPFv3

Usage By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. This command differentiates high-bandwidth links from lower-bandwidth links. If multiple links have high bandwidth, specify a larger reference bandwidth so that the cost of those links is differentiated from the cost of lower-bandwidth links.

bfd

Description Enable BFD on all interfaces for which OSPF is running.

Syntax

```
[no] bfd all-interfaces
```

Default Disabled

Mode OSPFv2 or OSPFv3

clear

Description Clear all or specific OSPF neighbors.

Syntax

```
clear ip ospf [process-id]
{
process |
neighbor
  {all | neighbor-id | interface
    {interface-ip-address [neighbor-ip-address]}}
}

clear ipv6 ospf [process-tag]
{
process |
neighbor
  {all | neighbor-id |
     interface-name [neighbor-id]}
}
```

Parameter	Description
process-id	Specifies the IPv4 OSPFv2 process to run on the device, and can be 1-65535.
process-tag	Specifies the IPv6 OSPFv3 process to run on the IPv6 link, and can be 1-65535.
neighbor-id	Router-id of the OSPF device.
neighbor-ip-address	IP address of the interface for the neighboring device.
interface-ip-address	IP address of the interface of the device on which the OSPF neighbor exists.

Default N/A

Mode OSPFv2 or OSPFv3

Usage Using OSPFv2, the CLI enables you to indicate an interface IP Address of the ACOS device. Using OSPFv3, the CLI enables you to specify the interface name for a specific neighbor.

Example The following command clears all OSPFv2 neighbors:

```
ACOS(config)#clear ip ospf neighbor all
```

Example The following command clears all neighbors to a specific router:

```
ACOS(config)#clear ip ospf neighbor 192.1.1.1
```

Example The following command clears all neighbors on an interface:

```
ACOS(config)#clear ip ospf neighbor interface 10.1.1.10
```

Example The following command clears a neighbor on a specified interface to a specified router:

```
ACOS(config)#clear ip ospf neighbor interface 10.1.1.10
192.1.1.10
```

Example The following command clears all OSPFv3 neighbors:

```
ACOS(config)#clear ipv6 ospf 5 neighbor all
```

Example The following command clears all neighbors to a specific router:

```
ACOS(config)#clear ipv6 ospf neighbor 192.1.1.1
```

Example The following command clears all OSPFv3 neighbors on a specified interface:

```
ACOS(config)#clear ipv6 ospf neighbor ethernet 1
```

Example The following command clears all neighbors on a specified interface to a specific router:

```
ACOS(config)#clear ipv6 ospf neighbor ethernet 1 192.1.1.1
```

default-information originate

Description Create a default route into the OSPF domain.

Syntax

```
[no] default-information originate
[always]
[metric num]
[metric-type {1 | 2}]
[route-map name]
```

Parameter	Description
always	Configures the ACOS device to automatically declare itself a default gateway for other OSPF routers, even if the ACOS device does not have a default route to

Parameter	Description
	0.0.0.0/0.
metric *num*	Metric for the default route, 0-16777214.
metric-type {**1** | **2**}	External link type associated with the default route advertised into the OSPF routing domain: • 1 - Type 1 external route. • 2 - Type 2 external route.
route-map *map-name*	Name of a route-map

Default This option is disabled by default. If you enable it, the default metric is 10. The default metric type is 2.

Mode OSPFV2 and OSPFV3

Usage When default-information originate is configured under OSPF, an external LSA for default route is generated if the Routing Information Base has a default route.

Example The following command creates a default route into the OSPF domain with a metric of 20:

```
ACOS(config-router)# default-information originate metric 20
```

default-metric

Description Set the numeric cost that is assigned to OSPF routes by default. The metric (cost) is added to routes when they are redistributed.

Syntax

```
[no] default-metric num
```

Replace *num* with the default cost, 0-16777214.

Default 20

Mode OSPFv2 or OSPFv3

Example The following command configures a default metric of 6666:

```
ACOS(config-router)#default-metric 6666
```

distribute-internal

Description Enable redistribution of ACOS-specific resources as internal routes (type-1 LSAs).

Syntax

```
[no] distribute-internal
{lw4o6 [options] | floating-ip | ip-nat | ip-nat-list | vip |
vip-only-flagged} area area-id [cost num]
```

Default Distribute-internal for router IPv6 OSPF:

Syntax

```
[no] distribute-internal
{lw4o6 [options] | nat64 | floating-ip | ip-nat | ip-nat-list
| vip | vip-only-flagged}
```

Parameter	Description
lw4o6 *[options]*	Redistributes LW4o6 routes into OSPF.
nat64	Redistributes NAT64 routes into OSPF.
floating-ip *[options]*	Redistributes routes into OSPF for reaching floating IP addresses.
ip-nat	Redistributes routes into OSPF for reaching translated NAT addresses allocated from a pool.
ip-nat-list	Redistributes routes into OSPF for reaching translated NAT addresses allocated from a range list.
vip	Redistributes routes into OSPF for reaching virtual server IP addresses.
vip-only-flagged	Same as the vip option, but applies only to VIPs on which the redistribution-flagged option is enabled.

Default Disabled. By default, OSPF routes are not redistributed. For other defaults, see above.

Mode OSPFv2 or OSPFv3

Usage Routes that are redistributed into OSPF as external routes are redistributed as type-5 link state advertisement (LSAs). Routes that are redistributed into OSPF as internal routes are redistributed as type-1 LSAs.

You can enable either external or internal redistribution for a given ACOS-specific resource type.

Example The following command enables internal distribution into OSPF area 0, of routes to all VIPs configured on the ACOS device, and assigns cost 11 to the routes:

```
ACOS(config-router)#distribute-internal vip area 0 cost 11
```

Example The following command enables internal distribution into OSPF area 1, of routes to VIPs that have the redistribution-flagged option, and assigns cost 21 to the routes:

```
ACOS(config-router)#distribute-internal vip-only-flagged area
1 cost 21
```

Example The following command enables internal distribution into OSPF area 5, of routes to floating IP addresses, and assigns cost 555 to the routes:

```
ACOS(config-router)#distribute-internal floating-ip area 5
cost 555
```

Example The following command displays the OSPF IPv4 route table. The routes configured for internal distribution are indicated by “internal”.

```
ACOS(config-router)#show ip ospf route

OSPF process 11:  counter = 6
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  6.1.1.0/24 [10] is directly connected, ve 6, Area 0.0.0.0
C  111.1.1.2/32 [21] is directly connected, internal vip-only-
flagged, Area 0.0.0.1
```

```
C   111.1.1.3/32 [11] is directly connected, internal vip, Area
0.0.0.0
C   114.1.1.1/32 [21] is directly connected, internal vip-only-
flagged, Area 0.0.0.1
C   200.1.1.2/32 [555] is directly connected, internal
floating-ip, Area 0.0.0.5
```

ha-standby-extra-cost

Description Enable OSPF awareness of VRRP-A.

Syntax

```
[no] ha-standby-extra-cost cost [group group-num]
```

Parameter	Description
cost	Extra cost to add to the ACOS device's OSPF interfaces, if the VRRP-A status of one or more of the device's VRIDs is Standby (1-65535). If the resulting cost value is more than 65535, the cost is set to 65535.
group-num	A specific VRRP-A VRID that will incur the specified *cost*; if none are specified, all VRIDs will incur the extra *cost*. **NOTE:** This option is only available for OSPFv2.

Default Not set. The OSPF protocol on the ACOS device is not aware of the VRRP-A state (Active or Standby) of the ACOS device.

Mode OSPFv2 or OSPFv3

Usage Enter the command on each of the ACOS devices in the VRRP-A VRID..

log-adjacency-changes

Description Log changes in adjacency state.

Syntax

```
log-adjacency-changes {detail | disable}
```

Parameter	Description
detail	Enable the logging of all changes in adjacency state.
disable	Disable logging.

Default Logging is enabled in brief mode by default.

Mode OSPFv3

Usage In brief mode, the following state changes are logged:

- FULL -> XXXX
- XXXX -> FULL
- XXXX -> DOWN

In **detail** mode, all state changes will be logged. In **disable** mode, no state changes are logged.

Example Enable the logging of all adjacency state changes.

```
ACOS(config)#router ipv6 ospf 2
ACOS(config-ospf:2)#log-adjacency-changes detail
```

max-concurrent-dd

Description Set the maximum number of OSPF neighbors that can be processed concurrently during database exchange between this OSPF router and its OSPF neighbors.

Syntax

```
[no] max-concurrent-dd num
```

Replace *num* with the maximum number of neighbors that can be processed at the same time during database exchange. You can specify 1-65535.

Default Not set (no limit)

Mode OSPFv2 or OSPFv3

Usage This command is useful in cases where router performance is being adversely affected by processing of neighbor adjacencies.

passive-interface

Description Disable Link-State Advertisements (LSAs) from being sent on an interface.

Syntax

```
[no] passive-interface
{ethernet portnum | lif num | loopback num | ve ve-num}
```

Default LSAs are enabled. (No interfaces are passive.)

Mode OSPFv2 or OSPFv3

Example The following command configures a passive interface on the Virtual Ethernet (VE) interface on VLAN 3:

```
ACOS(config-router)#passive-interface ve 3
```

redistribute

Description Enable distribution of routes from other sources into OSPF.

Syntax

```
[no] redistribute
{
bgp [options] |
connected [options] |
floating-ip [options] |
ip-nat [ipaddr/mask-length
floating-IP-forward-address ipaddr] [options] |
ip-nat-list [options] |
isis [options] |
lw4o6 [options] |
ospf [process-id] [options] |
rip [options] |
static [options] |
vip [ipaddr floating-IP-forward-address ipaddr |
  {only-flagged | only-not-flagged}] [options]
}
```

Parameter	Description
bgp [options]	Redistributes routes into OSPF for reaching BGP.
connected [options]	Redistributes routes into OSPF for reaching directly connected networks.
floating-ip	Redistributes routes into OSPF for reaching floating IP addresses.

Parameter	Description
[options]	
ip-nat *[ipaddr /mask-length | floating-IP-forward-address ipaddr] [options]*	Redistributes routes into OSPF for reaching translated NAT addresses allocated from a pool. By default, the forward address for all redistributed NAT pool addresses is 0.0.0.0. To set a floating IP address as the forward address, use the ipaddr/mask-length] option to specify the NAT pool address. The floating-IP-forward-address ipaddr option specifies the forward address to use when redistributing the route to the NAT pool address.
ip-nat-list *[options]*	Redistributes routes into OSPF for reaching translated NAT addresses allocated from a range list.
isis *[options]*	Redistributes routes into OSPF for IS-IS.
lw406 *[options]*	Redistributes routes into OSPF for Lightweight 4over6. (This is an IPv6 Migration feature.)
ospf *[process-id] [options]*	Redistributes routes into this OSPFv2 process for reaching networks in another OSPFv2 process.
rip *[options]*	Redistributes routes into OSPF for RIP.
static *[options]*	Redistributes routes into OSPF for reaching networks through static routes.
vip *[***ipaddr floating-IP-forward-**	Redistributes routes into OSPF for reaching virtual server IP addresses. By default, the forward address for all redistributed VIPs is 0.0.0.0. To set a floating IP address as the forward address, use the ipaddr option to specify the

Parameter	Description
address *ipaddr* | {**only-flagged** | **only-not-flagged**}] [*options*]	VIP address. Use the **floating-IP-forward-address** option to specify the forward address to use when redistributing the route to the VIP. To control which VIPs are redistributed, use one of the following options: • **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used. • **only-not-flagged** – Redistributes all VIPs except those on which the **redistribution-flagged** command is used. • *options* - Optional parameters supported for the options above: • **metric-type** {**1** | **2**} – External link type associated with the route advertised into the OSPF routing domain (1 for Type 1 external route, or 2 for Type 2 external route). • **metric** *num* – Metric for the route, 0-16777214. The default is 20. • **route-map** *map-name* – Name of a route-map. • **tag** *num* – Includes the specified tag value in external Link-State Advertisements (LSAs). Inter-domain routers running Border Gateway Protocol (BGP) can be configured to make routing decisions based on the tag value. The tag value can be 0-4294967295. The default is 0.

Default Disabled. By default, OSPF routes are not redistributed. For other defaults, see above.

Mode OSPFv2 or OSPFv3

Usage

When you enable redistribution, routes to all addresses of the specified type are redistributed. You can use the **vip** option to control which routes to VIPs are redistributed into OSPF.

By default, the ACOS device uses 0.0.0.0 as the forward address in routes that are redistributed in OSPF type-5 link state advertisement (LSAs). In this case, other OSPF routers find a route to reach the ACOS device (which is acting as OSPF ASBR), then use the corresponding next-hop address as the next hop for the destination network. You can specify a floating IP address to use as the forward address, for individual NAT pools or VIPs. (See the syntax above.)

VIP Redistribution

You can exclude redistribution of individual VIPs using one or the other of the following methods.

- If more VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to allow to be redistributed, enter the following command: **redistribution-flagged**
  - At the configuration level for the OSPFv2 process or OSPFv3 process, enter the following command: **redistribute vip only-flagged**
- If fewer VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to exclude from redistribution, enter the following command: **redistribution-flagged**
  - At the configuration level for the OSPFv2 process or OSPFv3 process, enter either of the following commands: **redistribute vip only-not-flagged** or **redistribute vip**

NOTE: In the configuration, the **redistribute vip** command is automatically converted into the **redistribute vip only-not-flagged** command. When you display the configuration, it will contain the **redistribute vip only-not-flagged** command, not the **redistribute vip** command.

VIP Redistribution Usage Examples:

- If you have 10 VIPs and all of them need to be redistributed by OSPF, use the **redistribute vip** command at the configuration level for the OSPF process.
- If you have 10 VIPs but only 2 of them need to be redistributed, use the **redistribution-flagged** command at the configuration level for each of the 2 VIPs, then use the **redistribute vip only-flagged** command at the configuration level for the OSPFv2 process or OSPFv3 process.
- If you have 10 VIPs and need to redistribute 8 of them, use the **redistribution-flagged** command at the configuration level for the 2 VIPs that should not be redistributed. Enter the **redistribute vip only-not-flagged** command at the configuration level for the OSPFv2 process or OSPFv3 process. (In this case, alternatively, you could enter **redistribute vip** instead of **redistribute vip only-not-flagged**.)
- If the route map configured under slb is not defined then the prefix is not redistributed (implicit deny).

Example The following commands redistribute floating IP addresses and VIP addresses into OSPF:

```
ACOS(config-router)# redistribute floating-ip
ACOS(config-router)# redistribute vip
```

Example The following commands flag a VIP, then configure OSPF to redistribute only that flagged VIP. The other (unflagged) VIPs will not be redistributed.

```
ACOS(config)# slb virtual-server vip1
ACOS(config-slb vserver)# redistribution-flagged
ACOS(config-slb vserver)# exit
ACOS(config)# router ospf
ACOS(config-ospf)# redistribute vip only-flagged
```

Example The following command enables redistribution of VIPs, and sets tag value 555 to be included in external LSAs that advertise the route to the VIP:

```
ACOS(config-router)# redistribute vip metric-type 1 metric 1
tag 555
```

Example The following command enables redistribution using the route-map under the slb virtual server and view the routes

```
ACOS(config)# slb virtual-server v1 5.5.5.5
ACOS(config-slb vserver)# redistribute route-map RMAP
ACOS(config-slb vserver)# exit
```

router-id

Description Set the value used by this OSPF router to identify itself when exchanging route information with other OSPF routers.

Syntax

```
[no] router-id ipaddr
```

NOTE: The syntax for this command is slightly different for OSPFv2. See ospf router-id.

Default The default router ID is the highest-numbered IP address configured on any of the ACOS device's loopback interfaces. If no loopback interfaces are configured, the highest-numbered IP address configured on any of the ACOS device's other Ethernet data interfaces is used.

NOTE: Setting the router ID is required for OSPFv3 and is strongly recommended for OSPFv2.

Mode OSPFv2 or OSPFv3

Usage The ACOS device has only one router ID. The address does not need to match an address configured on the ACOS device. However, the address must be an IPv4 address and must be unique within the routing domain.

New or changed router IDs require a restart of the OSPF process. To restart the OSPF process, use the **clear ip ospf process** command.

Example The following commands set the router ID to 3.3.3.3 and reload OSPF to place the new router ID into effect:

```
ACOS(config)# router ospf
```

```
ACOS(config-ospf)# router-id 3.3.3.3
ACOS(config-ospf)# clear ip ospf process
```

timers spf exp

Description Change Shortest Path First (SPF) timers used for route recalculation following a topology change. This command enables exponential back-off delays for route recalculation.

Syntax

```
[no] timers spf exp min-delay max-delay
```

Parameter	Description
min-delay	Specifies the minimum number of milliseconds (ms) the OSPF process waits after receiving a topology change, before recalculating its OSPF routes. You can specify 0-2147483647.
max-delay	Specifies the maximum number of milliseconds (ms) the OSPF process waits after receiving a topology change, before recalculating its OSPF routes. You can specify 0-2147483647.

Default The default min-delay is 500 ms. The default max-delay is 50000 ms.

Mode OSPFv2 or OSPFv3

Usage After you enter this command, any pending route recalculations are rescheduled based on the new timer values.

router isis

address-family

Description Configure this IS-IS instance to exchange multicast IPv6 addresses with other IS-IS routers.

Syntax

```
[no] address-family ipv6
```

This command changes the CLI to the address-family configuration level, where the following commands are available.

Parameter	Description
adjacency-check	Enables IS-IS router adjacency based on Type-Length-Value (TLV) fields in IS-IS Hello packets between routers.
default-information originate	Enables advertisement of the default route in Link State Packets (LSPs) sent by this IS-IS instance.
distance	Sets the administrative distance, 1-255, for IS-IS routes.
exit-address-family	Exits from the address-family configuration level.
[**no**] **multi-topology** [**level-1** | **level-1-2** | **level-2**] [**transition**]	Enables multi-topology mode. The **transition** option accepts and generates both IS-IS IPv6 and multi-topology IPv6 TLVs.
redistribute *option*	Enables distribution of routes from other sources into IS-IS. For available options, see redistribute.
summary-prefix *ipv6-addr/prefix* [**level-1** | **level-1-2** | **level-2**]	Configures an IPv6 summary prefix.

Default Disabled. When you enable IPv6 exchange, the unicast option is disabled by default.

Mode IS-IS

Example The following command enables exchange of IPv6 multicast addresses with other IS-IS routers, and enables the default route to be advertised.

```
ACOS(config)#router isis
ACOS(config-isis)#address-family ipv6
ACOS(config-isis-ipv6)#default-information originate
```

adjacency-check

Description Enable IS-IS router adjacency based on Type-Length-Value (TLV) fields in IS-IS Hello packets between routers.

Syntax

```
[no] adjacency-check
```

Default Enabled.

Mode IS-IS

area-password

Description Configure the password for authenticating IS-IS traffic between Level-1 routers.

Syntax

```
[no] area-password string
[authenticate snp {send-only | validate}]
```

Parameter	Description
string	Specifies the password.
authenticate snp	Uses the password for authentication of Sequence Number Packets (SNPs).
send-only	Inserts the password into SNP PDUs before sending them, but does not check for the password in SNP PDUs received from other routers.
validate	Inserts the password into SNP PDUs before sending them, and also checks for the password in SNP PDUs received from other routers.

Default None. If you configure a Level-1 password, the **snp** option is disabled by default.

Mode IS-IS

Example The following command configures IS-IS to use password “isisl1pwd” to authenticate Level-1 IS-IS traffic within the area, including inbound and outbound SNP PDUs:

```
ACOS(config)#router isis
```

```
ACOS(config-isis)#area-password isisl1pwd authenticate snp
validate
```

Related Commands:

- domain-password

authentication

Description Configures authentication for this IS-IS instance.

Syntax

```
[no] authentication send-only [level-1 | level-2]
[no] authentication mode md5 [level-1 | level-2]
[no] authentication key-chain name [level-1 | level-2]
```

Parameter	Description
send-only [**level-1** | **level-2**]	Disables checking for keys in IS-IS packets received by this IS-IS instance. • **level-1** – Disables key checking only for Level-1 (intra-area) IS-IS traffic. • **level-2** – Disables key checking only for Level-2 (inter-area) IS-IS traffic.
mode md5 [**level-1** | **level-2**]	Enables MD5 authentication. • **level-1** – Enables MD5 only for Level-1 (intra-area) IS-IS traffic. • **level-2** – Enables MD5 only for Level-2 (inter-area) IS-IS traffic. **NOTE:** The **authentication mode md5** option is not supported in FIPS mode.
key-chain *name* [**level-1** | **level-2**]	Specifies the name of the certificate key chain to use for authenticating IS-IS traffic. • **level-1** – Applies only to Level-1 (intra-

Parameter	Description
	area) IS-IS traffic. • **level-2** – Applies only to Level-2 (inter-area) IS-IS traffic.

Default Clear-text authentication is enabled by default. MD5 authentication is disabled by default. No key chain is set by default. The **send-only** option is disabled by default. All options apply to Level-1 and Level-2, unless you specify one level or the other. For all options that accept the **level-1**, **level-1-2**, or **level-2** keyword, the default is **level-1**.

Mode IS-IS

Usage Use the **send-only** option to temporarily disable key checking, then use the **key-chain** option to specify the key chain. To use MD5, use the **md5** option to disable clear-text authentication and enable MD5 authentication. After key-chains are installed on the other IS-IS routers, disable the **send-only** option.

Example The following commands configure MD5 authentication for this IS-IS instance:

```
ACOS(config)#router isis
ACOS(config-isis)#authentication send-only
ACOS(config-isis)#authentication mode md5
ACOS(config-isis)#authentication key-chain chain1
ACOS(config-isis)#no authentication send-only
```

bfd

Description Enables BFD on all interfaces for which IS-IS is running.

Syntax `[no] bfd all-interfaces`

Default Disabled

Mode IS-IS

default-information originate

Description Enable advertisement of the default route in Link State Packets (LSPs) sent by this IS-IS instance.

Syntax

```
[no] default-information originate
```

Default Disabled

Mode IS-IS

Usage If the IPv4 or IPv6 data route tables contain a default route, the default route is included in Level-2 LSPs sent by this IS-IS instance. This command does not apply to Level-1 LSPs.

distance

Description Set the administrative distance for IS-IS routes.

Syntax

```
[no] distance num [ system-id ]
```

Parameter	Description
num	Specifies the distance, 1-255.
system-id	Assigns the distance only to routes from the router with the specified IS-IS system ID.

Default None

Mode IS-IS

Usage The administrative distance specifies the trustworthiness of routes. A low administrative distance value indicates a high level of trust. Likewise, a administrative distance value indicates a low level of trust. For example, setting the administrative distance value for external routes to 255 means those routes are very untrustworthy and should not be used.

domain-password

Description Configure the password for authenticating IS-IS traffic between Level-2 routers.

Syntax

```
[no] domain-password string
[authenticate snp {send-only | validate}]
```

Parameter	Description
string	Specifies the password.
authenticate snp	Uses the password for authentication of Sequence Number Packets (SNPs).
send-only	Inserts the password into SNP PDUs before sending them, but does not check for the password in SNP PDUs received from other routers.
validate	Inserts the password into SNP PDUs before sending them, and also checks for the password in SNP PDUs received from other routers.

Default None. If you configure a Level-2 password, the **snp** option is disabled by default.

Mode IS-IS

Example The following command configures IS-IS to use password “isisl2pwd” to authenticate Level-2 IS-IS traffic, including inbound and outbound SNP PDUs:

```
ACOS(config)#router isis
ACOS(config-router)#domain-password isisl2pwd authenticate snp
validate
```

Related Commands:

- domain-password

ha-standby-extra-cost

Description Enable IS-IS awareness of VRRP-A.

Syntax

```
[no] ha-standby-extra-cost num
```

Replace *num* with the extra cost to add to the ACOS device’s IS-IS interfaces, if the VRRP-A status of one or more of the device’s VRIDs is

Standby. You can specify 1-65535. If the resulting cost value is more than 65535, the cost is set to 65535.

Default Not set. The IS-IS protocol on the ACOS device is not aware of the VRRP-A state (Active or Standby) of the ACOS device.

Mode IS-IS

Usage Enter the command on each of the ACOS devices in the VRRP-A VRID.

key

Description Configure a key chain for use by RIP or IS-IS MD5 authentication.

Syntax

```
[no] key chain name
```

Replace *name* with the name of the key chain (1-31 characters).

This command changes the CLI to the configuration level for the specified key chain, where the following key-chain related command is available:

```
[no] key num
```

This command adds a key and enters configuration mode for the key. The key number can be 1-255. This command changes the CLI to the configuration level for the specified key, where the following key-related command is available:

```
[no] key-string string
```

This command configures the authentication string of the key, 1-16 characters.

Default By default, no key chains are configured.

Mode Global Config

Usage Although you can configure multiple key chains, it is recommends using one key chain per interface, per routing protocol.

Example The following commands configure a key chain named “example_chain”.

```
ACOS(config)# key chain example_chain
ACOS(config-keychain)# key 1
```

```
ACOS(config-keychain-key)# key-string thisiskey1
ACOS(config-keychain-key)# exit
ACOS(config-keychain)# key 2
ACOS(config-keychain-key)# key-string thisiskey2
ACOS(config-keychain-key)# exit
ACOS(config-keychain)# key 3
ACOS(config-keychain-key)# key-string thisiskey3
```

ignore-lsp-errors

Description Disable checksum verification for inbound LSPs.

Syntax `[no] ignore-lsp-errors`

Default Disabled. The checksums of inbound LSPs are verified.

Mode IS-IS

is-type

Description Specify the IS-IS routing level for this IS-IS instance.

Syntax `[no] is-type {level-1 | level-1-2 | level-2-only}`

Parameter	Description
`level-1`	Level-1 (intra-area) only.
`level-1-2`	Level-1 and Level-2.
`level-2-only`	Level-2 (inter-area) only.

Default Level-1.

Mode IS-IS

Usage Only one IS-IS instance on the ACOS device can run Level-2 routing.

log-adjacency-changes

Description Log adjacency changes.

Syntax `[no] log-adjacency-changes {detail | disable}`

Parameter	Description
detail	Log changes in adjacency state.
disable	Disable logging of adjacency state changes.

Default Enabled by default.

Mode IS-IS

Example The following example disables logging of adjacency state changes:

```
ACOS(config)#router isis
ACOS(config-isis)#log-adjacency-changes disable
```

lsp-gen-interval

Description Configure the minimum interval for LSP regeneration.

Syntax `[no] lsp-gen-interval seconds [level-1 | level-2]`

Parameter	Description
level-1 | **level-2**	Specifies the circuit type to which to apply the interval configuration. The default is **level-1**.
seconds	Specifies the minimum number of seconds between each regeneration of the LSP. You can specify 1-120 seconds.

Default 30 seconds, for both Level-1 and Level2

Mode IS-IS

lsp-refresh-interval

Description Configure the LSP refresh interval.

Syntax `[no] lsp-refresh-interval seconds`

Replace *seconds* with the minimum number of seconds IS-IS must wait before refreshing an LSP. You can specify 1-65535 seconds.

Default 900

Mode IS-IS

Usage The **lsp-refresh-interval** must be smaller than the max-lsp-lifetime.

max-lsp-lifetime

Description Configure the LSP maximum lifetime.

Syntax

```
[no] max-lsp-lifetime seconds
```

Replace *seconds* with the maximum number of seconds an LSP can remain in the database without being refreshed. You can specify 350-65535 seconds.

Default 1200

Mode IS-IS

Usage The **max-lsp-lifetime** must be larger than the lsp-refresh-interval.

metric-style

Description Configure the metric style to use for SPF calculation and for TLV encoding in LSPs.

Syntax

```
[no] metric-style
{
narrow [[level-1 | level-1-2 | level-2]] |
transition [level-1 | level-1-2 | level-2] |
wide [[level-1 | level-1-2 | level-2] |
narrow-transition [level-1 | level-1-2 | level-2] |
wide-transition [level-1 | level-1-2 | level-2]}
```

Parameter	Description
narrow	Supports 6-bit metric length for SPF calculation and TLV encoding. The **transition** option also allows 24-bit metrics for SPF calculation, but not for TLV encoding. • **level-1** – Supports 24-bit SPF calculation only for circuit type Level-1.

Parameter	Description
	• **level-2** – Supports 24-bit SPF calculation only for circuit type Level-2. • **level-1-2** – Supports 24-bit SPF calculation for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)
transition	Supports 6-bit and 24-bit metric lengths for SPF calculation and TLV encoding. • **level-1** – Supports both metric lengths only for circuit type Level-1. • **level-2** – Supports both metric lengths only for circuit type Level-2. • **level-1-2** – Supports both metric lengths for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)
wide	Supports 24-bit metric length for SPF calculation and TLV encoding. The **transition** option also allows 6-bit metrics for SPF calculation, but not for TLV encoding. • **level-1** – Supports 6-bit SPF calculation only for circuit type Level-1. • **level-2** – Supports 6-bit SPF calculation only for circuit type Level-2. • **level-1-2** – Supports 6-bit SPF calculation for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.) This command should be included in all IPv6 IS-IS configurations.

Parameter	Description
narrow-transition	Supports 6-bit metric length for SPF calculation and TLV encoding. The **transition** option also allows 24-bit metrics for SPF calculation, but not for TLV encoding. • **level-1** – Supports 24-bit SPF calculation only for circuit type Level-1. • **level-2** – Supports 24-bit SPF calculation only for circuit type Level-2. • **level-1-2** – Supports 24-bit SPF calculation for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)
wide-transition	Supports 24-bit metric length for SPF calculation and TLV encoding. The **transition** option also allows 6-bit metrics for SPF calculation, but not for TLV encoding. • **level-1** – Supports 6-bit SPF calculation only for circuit type Level-1. • **level-2** – Supports 6-bit SPF calculation only for circuit type Level-2. • **level-1-2** – Supports 6-bit SPF calculation for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)

Default Narrow, for Level-1 and Level-2 routing levels (**level-1-2**). For all options that accept the **level-1**, **level-1-2**, or **level-2** keyword, the default is **level-1**.

Mode IS-IS

net

Description Configure a Network Entity Title (NET) for the instance.

Syntax

```
[no] net area-address.system-id.00
```

Parameter	Description
area-address	Specifies the address of the IS-IS area.
system-id	Specifies the system ID.

Default None

Mode IS-IS

Usage Each IS-IS instance must have at least 1 NET.

The total length of the NET can be 8-20 bytes.

- The last (right-most) byte must be 00.
- The *system-id* must be 6 bytes long. For Level-1, the *system-id* must be unique within the area. For Level-2, the *system-id* must be unique within the entire domain.
- The *area-address* can be up to 13 bytes long.

You can configure more than one NET. This is useful in cases where you are reconfiguring the network and need to temporarily merge or split existing areas.

If you configure more than 1 NET, the *area-address* must be unique in each NET but the *system-id* must be the same.

passive-interface

Description Disable routing IS-IS routing updates on ACOS interfaces.

Syntax

```
[no] passive-interface
{ethernet num | lif num | loopback num | trunk num | ve ve-num}
```

Parameter	Description
ethernet	Disables routing updates from being sent on the

Parameter	Description
num	specified Ethernet data port.
lif *num*	Disables routing updates from being sent on the specified logical interface.
loopback *num*	Disables routing updates from being sent on the specified loopback interface.
trunk *num*	Disables routing updates from being sent on the specified trunk interface.
ve *ve-num*	Disables routing updates from being sent on the specified Virtual Ethernet (VE) interface.

Default Disabled

Mode IS-IS

Usage This command removes all IS-IS configuration from the specified interface.

For proper operation of IS-IS, routing updates must be enabled on at least one interface.

protocol-topology

Description Enable IS-IS protocol topology support, which provides IPv4/IPv6/dual-stack support.

Syntax

```
[no] protocol-topology
```

Default Disabled

Mode IS-IS

Usage For standard IS-IS support, leave this option disabled.

redistribute

Description Enable distribution of routes from other sources into IS-IS.

Syntax

```
[no] redistribute
{
bgp [options] |
connected [options] |
```

```
floating-ip [options] |
ip-nat [options] |
ip-nat-list [options] |
isis [options] |
lw4o6 [options] |
ospf [process-id] [options] |
rip [route-map map-name] |
static [options] |
vip [only-flagged | only-not-flagged] [options]
}
```

Parameter	Description
bgp [*options*]	Redistributes route information from Border Gateway Protocol (BGP) into IS-IS.
connected [*options*]	Redistributes routes into IS-IS for reaching directly connected networks.
floating-ip [*options*]	Redistributes routes into IS-IS for reaching floating IP addresses.
ip-nat [*options*]	Redistributes routes into IS-IS for reaching translated NAT addresses allocated from a pool.
ip-nat-list [options]	Redistributes routes into IS-IS for reaching translated NAT addresses allocated from a range list.
isis [*options*]	Redistributes routes back into IS-IS.
lw406 [*options*]	Redistributes routes into IS-IS for Lightweight 4over6. (This is an IPv6 Migration feature.)
ospf [*process-id*] [*options*]	Redistributes OSPF routes into IS-IS.
rip [*options*]	Redistributes routes into IS-IS for RIP.
static [*options*]	Redistributes routes into IS-IS for reaching networks through static routes.
vip [only-flagged | only-not-flagged] [options]	TO control which VIPs are redistributed, use one of the following options: • **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used. • **only-not-flagged** – Redistributes all VIPs

Parameter	Description
	except those on which the **redistribution-flagged** command is used.
[options]	Optional parameters supported for all other options in this table: • **level-1** – Redistributes only at the IS-IS area level. (This is the default IS-IS level.) • **level-1-2** – Redistributes at both the IS-IS area and domain levels. • **level-2** – Redistributes only at the IS-IS domain level. (This is the default.) • **metric** *num* – Metric for the default route, 0-4261412864. The default is 0. • **metric-type** – Specifies the metric information used when comparing the route to other routes: ◦ The **external** type uses the route's metric for comparison. ◦ The **internal** type uses the route's metric for comparison and also uses the cost of the router that advertised the route (this is the default). • **route-map** *map-name* – Name of a route-map.

Default Disabled. By default, IS-IS routes are not redistributed. For other defaults, see above.

Mode IS-IS

Usage When you enable redistribution, routes to all addresses of the specified type are redistributed. Use the **vip** option to control which routes to VIPs are redistributed into IS-IS.

VIP Redistribution

You can exclude redistribution of individual VIPs using one or the other of the following methods.

- If more VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to allow to be redistributed, enter the following command: **redistribution-flagged**
  - At the configuration level for IS-IS, enter the following command: **redistribute vip only-flagged**
- If fewer VIPs will be excluded than will be allowed to be redistributed:
  - At the configuration level for each of the VIPs to exclude from redistribution, enter the following command: **redistribution-flagged**
  - At the configuration level for IS-IS, enter either of the following commands: **redistribute vip only-not-flagged** or **redistribute vip**

NOTE: In the configuration, the **redistribute vip** command is automatically converted into the **redistribute vip only-not-flagged** command. When you display the configuration, it will contain the **redistribute vip only-not-flagged** command, not the **redistribute vip** command.

VIP Redistribution Usage Examples:

- If you have 10 VIPs and all of them need to be redistributed by IS-IS, use the **redistribute vip** command at the configuration level for IS-IS.
- If you have 10 VIPs but only 2 of them need to be redistributed, use the **redistribution-flagged** command at the configuration level for each of the 2 VIPs, then use the **redistribute vip only-flagged** command at the configuration level for IS-IS.
- If you have 10 VIPs and need to redistribute 8 of them, use the **redistribution-flagged** command at the configuration level for the 2 VIPs that should not be redistributed. Enter the **redistribute vip only-not-flagged** command at the

configuration level for IS-IS. (In this case, alternatively, you could enter **redistribute vip** instead of **redistribute vip only-not-flagged**.)

Example The following commands redistribute floating IP addresses and OSPF routes into IS-IS:

```
ACOS(config)#router isis
ACOS(config-isis)#redistribute floating-ip
ACOS(config-isis)#redistribute ospf
```

set-overload-bit

Description Disable use of this IS-IS router as a transit router during SPF calculation.

Syntax

```
[no] set-overload-bit
```

Syntax

```
[no] set-overload-bit on-startup {seconds | wait-for-bgp}
```

Syntax

```
[no] set-overload-bit suppress {[external] [interlevel]}
```

Parameter	Description
on-startup {*seconds* | **wait-for-bgp**}	Sets the overload bit only after startup of the IS-IS instance, and clears the bit based on one of the following options: • seconds – Clears the overload bit after the specified number of seconds. You can specify 5-86400 seconds. • wait-for-bgp – Clears the overload bit after BGP signals that it has finished convergence. ◦ If BGP is not running, the overload bit is immediately cleared. ◦ If BGP is running but does not signal convergence within 10 minutes after the IS-IS instance starts, the overload bit is cleared.

Parameter	Description
supress {**external** | **interlevel**}	Suppresses redistribution of specific types of reachability information during the overload state. • external – Suppresses redistribution of IP prefixes learned from other protocols. For example, redistribution of IP prefixes from OSPF is suppressed. • interlevel – Suppresses redistribution of IP prefixes learned from other IS-IS levels. For example, redistribution of IP prefixes from Level-2 to Level-1 is suppressed.

Default Disabled. The overload bit is not set, and this IS-IS router can be used as a transit (intermediate hop) router during SPF calculation.

Mode IS-IS

Usage IP prefixes that are directly connected to this IS-IS router continue to be reachable even when the overload bit is set.

spf-interval-exp

Description Configure the minimum and maximum delay between receiving a link-state or IS-IS configuration change, and SPF recalculation.

Syntax `[no] spf-interval-exp min-delay max-delay [level-1 | level-2]`

Parameter	Description
level-1 | **level-2**	Specifies the IS-IS level to which to apply the interval setting. The default is `level-1`.
min-delay	Specifies the minimum number of milliseconds (ms) to wait before SPF recalculation following a link-state or IS-IS configuration change. You can specify 0-2147483647 ms.

Parameter	Description
max-delay	Specifies the maximum number of ms to wait. You can specify 0-2147483647 ms.

Default The default *min-delay* is 500 ms and the default *max-delay* is 50000 ms, for Level-1 and Level-2 routing levels.

Mode IS-IS

summary-address

Description Configure an IPv4 summary address to aggregate multiple IPv4 prefixes for advertisement.

Syntax

```
[no] summary-address ipaddr/mask-length
[level-1 | level-1-2 | level-2]
```

Parameter	Description
ipaddr **/***mask-length*	Specifies the summary IPv4 address to advertise.
level-1 | **level-1-2** | **level-2**	Specifies the IS-IS routing level to which to advertise the summary address. If you do not specify a routing level, the summary address is advertised at Level-2 only.

Default None

Mode IS-IS

Usage The summary address is advertised instead of the individual IP prefixes contained in the summary address. For example, if the IPv4 route table has routes to 192.168.1.x/24, 192.168.2.x/24, and 192.168.11.x/24, you can configure IS-IS to advertise summary address 192.168.0.0/16 instead of each of the individual prefixes.

router bgp

To access the BGP router configuration level, use the **router bgp** command at the global configuration level of the CLI:

```
ACOS(config)#router bgp 100
ACOS(config-bgp:100)#
```

address-family

Description Configure address family parameters.

Syntax

```
[no] address-family ivp6
```

Parameter	Description
[no] **aggregate-address** *options*	See aggregate-address.
[no] **auto-summary**	See auto-summary.
[no] bgp **dampening** *options*	See bgp dampening.
[no] **default-information originate**	See default-information originate.
[no] **distance**	See distance.
[no] **exit-address-family**	Exits the address-family configuration level.
[no] **maximum-paths**	See maximum-paths.

Parameter	Description
[**no**] **neighbor** *options*	neighbor neighbor-id activate

Parameter	Description
	neighbor neighbor-id advertisement-interval
	neighbor neighbor-id allowas-in
	neighbor neighbor-id as-origination-interval
	neighbor neighbor-id capability
	neighbor neighbor-id collide-established
	neighbor neighbor-id description
	neighbor neighbor-id dont-capability-negotiate
	neighbor neighbor-id ebgp-multihop
	neighbor neighbor-id enforce-multihop
	neighbor neighbor-id fall-over
	neighbor neighbor-id maximum-prefix
	neighbor neighbor-id override-capability
	neighbor neighbor-id passive
	neighbor neighbor-id password
	neighbor neighbor-id peer-group
	neighbor neighbor-id remote-as
	neighbor neighbor-id remove-private-as
	neighbor neighbor-id route-map
	neighbor neighbor-id send-community
	neighbor neighbor-id shutdown
	neighbor neighbor-id soft-reconfiguration
	neighbor neighbor-id strict-capability-

Parameter	Description
	match
	neighbor neighbor-id timers
	neighbor neighbor-id update-source
	neighbor neighbor-id weight
	neighbor <ip-addr | ipv6-addr> capability graceful-restart
[no] **network** *options*	See network.
[no] **nexthop** *options*	See nexthop.
[no] **redistribute** *options*	See redistribute.

Default None

Mode BGP

aggregate-address

Description Configure an aggregate address.

Syntax

```
[no] aggregate-address ipaddr/mask-length [as-set] [summary-only]
```

Parameter	Description
ipaddr **/***mask-length*	If you are using this command at the BGP configuration level, specify an IPv4 aggregate network address. If you are using the command at the address-family configuration level, you must specify an IPv6 IP aggregate network address.
as-set	Generates AS set path information.
summary-only	Filters more specific routes from updates.

Default None

Mode BGP or address-family

auto-summary

Description Enable sending of summarized routes to BGP peers.

Syntax

```
[no] auto-summary
```

Default Disabled

Mode BGP

bgp always-compare-med

Description Enable comparison of the Multi Exit Discriminators (MEDs) for paths from neighbors in different ASs.

Syntax

```
[no] bgp always-compare-med
```

Default Disabled. By default, MED comparison is done only among paths from the same AS.

Mode BGP

bgp bestpath

Description Configure options to select the best of multiple paths for a route.

Syntax

```
[no] bgp bestpath { as-path [ignore] | compare-routerid }
```

Parameter	Description
as-path	Use the AS path when selecting the best path for a route. AS path consideration is enabled by default.
ignore	Ignore the AS path when selecting the best path for a route.
compare-routerid	Enables comparison of router IDs when comparing identical routes received from different neighbors. In this case, the route from the neighbor with the

Parameter	Description
	lowest route ID is selected. By default, BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Mode BGP

bgp dampening

Description Configure the BGP response to route flapping, to minimize network disruption.

Syntax

```
[no] bgp dampening { dampening-options | route-map map-name }
```

Parameter	Description
dampening-options	Configures the dampening options: • reachability-half-life—Specifies the reachability half-life, which is the time it takes the penalty to decrease to one-half of its current value. You can specify 1-45 minutes. The default is 15 minutes. • reuse-start—Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. You can specify 1-20000. The default is 750. • suppress-start—Specifies the suppress limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. You can specify 1-20000. The default is 2000.

Parameter	Description
	• max-suppress-duration—Specifies the maximum time that a dampened route is suppressed. You can specify 1-255 minutes. The default is 60 minutes (4 times the half-life time).
map-name	Applies the dampening settings only to routes that match the specified route map.

Default See descriptions.

Mode BGP

bgp default

Description Change BGP default settings.

Syntax `[no] bgp default {ipv4-unicast | local-preference num }`

Parameter	Description
ipv4-unicast	Activates IPv4 unicast for communication with peers. By default, this is enabled.
num	Specifies the local preference value for routes. You can specify 0-4294967295. The default is 100.

Default See descriptions.

Mode BGP

bgp deterministic-med

Description Enable comparison of the Multi Exit Discriminator (MED) values during selection of a route among routes advertised by different peers in the same AS.

Syntax `[no] bgp deterministic-med`

Default Disabled

Mode BGP

bgp enforce-first-as

Description Enable the ACOS device to deny any updates received from an external neighbor that do not have the neighbor's configured AS at the beginning of the AS_PATH.

Syntax `[no] bgp enforce-first-as`

Default Enabled

Mode BGP

bgp fast-external-failover

Description Enable immediate reset of a BGP session if the interface used for the BGP connection goes down.

Syntax `[no] bgp fast-external-failover`

Default Enabled

Mode BGP

bgp graceful-restart

Description Enable the GR helper mode and use default value for both the timers. Enable the configuration for both the timer and neighbor. See neighbor <ip-addr | ipv6-addr> capability graceful-restart to enable the configuration.

Syntax `bgp graceful-restart [restart-time <1-3600>] [stalepath-time <1-3600>]`

Parameter	Description
`restart-time`	BGP peer graceful restart time in seconds.

Parameter	Description
stalepath-time	BGP graceful restart stalepath retention time in seconds.

Default The default restart time is 90 seconds. The default stalepath time 360 seconds.

Mode BGP

bgp log-neighbor-changes

Description Enable logging of status change messages without enabling BGP debugging.

Syntax `[no] bgp log-neighbor-changes`

Default Disabled

Mode BGP

bgp nexthop-trigger-count

Description Configure display of BGP nexthop-tracking status.

Syntax `[no] bgp nexthop-trigger-count num`

Parameter	Description
num	Count value (0-127).

Mode BGP

bgp router-id

Description Configure the router ID.

Syntax `[no] bgp router-id ipaddr`

Parameter	Description
ipaddr	IPv4 address.

Default If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If there are multiple loopback interfaces, the loopback interface with the highest numbered IP address is used.

If there are no loopback interfaces, the interface with the highest numbered IP address is used.

Mode BGP

bgp scan-time

Description Set the interval for BGP route next-hop scanning.

Syntax

```
[no] bgp scan-time seconds
```

Parameter	Description
seconds	Amount of time between scans, in seconds (0-60 seconds).

Default 60

Mode BGP

default-information originate

Description Enable advertisement of the default route in packets sent by this BGP instance.

A valid default route must exist and be verified to complete this configuration or the default route will not be advertised

Syntax

```
[no] default-information originate
```

Default Disabled

Mode BGP

distance

Description Configure the administrative distance for BGP. The administrative distance is a rating of trustworthiness of the BGP process relative to other routing processes running on the ACOS device. The greater the distance, the lower the trust rating.

Syntax

```
[no] distance
{ admin-distance ipaddr/mask-length [acl-id] | bgp external
internal local }
```

Parameter	Description
admin-distance *ipaddr* */mask-length* *[acl-id]*	Overrides the configured administrative distance for specific prefixes. The *acl-id* option specifies an ACL that matches on the routes for which to override the default administrative distance. If you do not use this option, the distance is applied to all IPv4 BGP routes. **NOTE:** This option is not available if you are configuring the distance at the address-family configuration level.
bgp *external* *internal* *local*	• *external* – Specifies the administrative distance (1-255) for BGP routes learned from another AS. The default external administrative distance is 20. • *internal* – Specifies the administrative distance (1-255)for BGP routes learned from a neighbor within the same AS. The default internal administrative distance is 200. • *local* – Specifies the administrative distance (1-255) for BGP routes redistributed from another route source on this ACOS device. The default local administrative distance is 200.

Default See descriptions.

Mode BGP

maximum-paths

Description Specify the maximum number of ECMP paths to a given route destination allowed for BGP.

For more information, refer 'Equal-Cost Multi-path ECMP Support' in *Network Configuration Guide*.

Syntax

```
[no] maximum-paths path-num
```

Parameter	Description
num	Maximum number of paths to a given destination. You can specify 1-64.

Default BGP will install the single best ECMP route into the FIB used by the ACOS device to forward traffic.

Mode BGP

neighbor neighbor-id activate

Description Enable the exchange of address family routes with a neighboring BGP router.

Syntax

```
[no] neighbor neighbor-id activate
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default N/A

Mode BGP

Usage After the TCP connection is opened with the neighbor, use this command to enable or disable the exchange of address family information with the neighboring router.

neighbor neighbor-id advertisement-interval

Description Configure the minimum interval between transmission of BGP route updates to a neighbor.

Syntax

```
[no] neighbor neighbor-id advertisement-interval seconds
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
seconds	Minimum interval between route updates. You can specify 0-600 seconds.

Default The advertisement interval has the following default settings:

- eBGP – 30 seconds
- iBGP – 5 seconds

Mode BGP

neighbor neighbor-id allowas-in

Description Allow re-advertisement of all prefixes containing duplicate AS numbers.

Syntax

```
[no] neighbor neighbor-id allowas-in [occurrences]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values:

Parameter	Description
	• IPv4 address. • IPv6 address. • Name of a peer group.
occurrences	Maximum number of occurrences of a given AS number. You can specify 1-10.

Default Disabled

Mode BGP

neighbor neighbor-id as-origination-interval

Description Configure the interval between transmission of AS origination route updates.

Syntax `[no] neighbor neighbor-id as-origination-interval seconds`

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
seconds	Time between AS origination route updates. You can specify 1-600 seconds.

Default 15 seconds

Mode BGP

neighbor neighbor-id capability

Description Configure capability settings for the ACOS device's BGP communication with a neighbor.

Syntax

```
[no] neighbor neighbor-id capability
{dynamic | orf prefix-list {both | receive | send} | route-
refresh}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
dynamic	Enables the ACOS device to advertise or withdraw an address family capability with the neighbor, without bringing down the BGP session with the peer.
orf prefix-list {both | receive | send}	Enables Outbound Router Filtering (ORF) and advertises the ACOS device's ORF capability to the neighbor. • both – ACOS device can send ORF entries to the neighbor, as well as receive ORF entries from the neighbor. • receive – ACOS device can receive ORF entries from the neighbor, but cannot send ORF entries to the neighbor. • send – ACOS device can send ORF entries to the neighbor, but cannot receive ORF entries from the neighbor.
route-refresh	Enables advertisement of route-refresh capability to the neighbor. When this option is enabled, the ACOS device can dynamically request the neighbor to re-advertise its Adj-RIB-Out.

Default None. (This assumes that the neighbor has no special capabilities or functions.)

Mode BGP

Usage BGP neighbors exchange ORFs reduce the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

The local router (ACOS device) advertises the ORF capability in send mode, and the remote router receives the ORF capability in receive mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each router. Only an individual router or a peer group can be configured to be in receive or send mode. A peer-group member cannot be configured to be in receive or send mode.

neighbor neighbor-id collide-established

Description Include the neighbor, if already in TCP established state, in conflict resolution if a TCP connection collision is detected.

Syntax

```
[no] neighbor neighbor-id collide-established
```

Replace *neighbor-id* with the ID of the neighbor, which can be one of the following types of values:

- *ipv4ipaddr* – IPv4 address.
- *ipv6addr* – IPv6 address.
- *tag* – Name of a peer group.

Default Use this command only if necessary. Generally, the command is not required.

Inclusion of a neighbor with an established TCP connection into resolution of TCP connection collision conflicts is automatically enabled when the neighbor is configured for BGP.

Mode BGP

neighbor neighbor-id default-originate

Description Enable transmission of a default route (0.0.0.0) to a neighbor.

Syntax

```
[no] neighbor neighbor-id default-originate [route-map map-name]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
map-name	Route map that specifies the nexthop IP address.

Default Disabled

Mode BGP

neighbor neighbor-id description

Description Configure a description for a neighbor.

Syntax

```
[no] neighbor neighbor-id description string [string ...]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
string	String that describes the neighbor (up to 80 characters).

Default None

Mode BGP

neighbor neighbor-id disallow-infinite-holdtime

Description Disallow a neighbor to set the holdtime to “infinite” (0 seconds).

Syntax

```
[no] neighbor neighbor-id disallow-infinite-holdtime
```

Replace *neighbor-id* with the ID of the neighbor, which can be one of the following types of values:

- *ipv4ipaddr* – IPv4 address.
- *ipv6addr* – IPv6 address.
- *tag* – Name of a peer group.

Default Disabled. Infinite holdtime is allowed.

Mode BGP

neighbor neighbor-id distribute-list

Description Filter route updates to or from a neighbor.

Syntax

```
[no] neighbor neighbor-id distribute-list ip-access-list {in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
ip-access-list	Time between AS origination route updates. You can specify 1-600 seconds.
in | **out**	Specifies the update direction to filter: • in – Updates received from the neighbor are filtered. • out – Updates sent to the neighbor are filtered before transmission.

Default None. By default, updates are not filtered.

Mode BGP

neighbor neighbor-id dont-capability-negotiate

Description Disable capability negotiation with a neighbor.

Syntax

```
[no] neighbor neighbor-id dont-capability-negotiate
```

Replace *neighbor-id* with the ID of the neighbor, which can be one of the following types of values:

- *ipv4ipaddr* – IPv4 address
- *ipv6addr* – IPv6 address
- *tag* – Name of a peer group

Default Capability negotiation is enabled by default.

Mode BGP

neighbor neighbor-id ebgp-multihop

Description Allow BGP connections with external peers on indirectly connected networks.

Syntax

```
[no] neighbor neighbor-id ebgp-multihop [count]
```

Parameter	Description
neighbor	The IPv4 or IPv6 address of the neighbor router, or the router tag (1-128 characters).
count	The maximum hop count to reach the neighbor (1-255). If no *count* is specified, the default hop count is 1.

Replace *count* with the maximum number of hops allowed, 1-255.

Default Disabled by default.

Mode BGP

neighbor neighbor-id enforce-multihop

Description Enforce eBGP neighbors to perform multihop.

Syntax `[no] neighbor neighbor-id enforce-multihop`

Default Enabled

Mode BGP

neighbor neighbor-id fall-over

Description Enable neighbor fall-over detection.

Syntax `[no] neighbor neighbor-id fall-over bfd`

Mode BGP

neighbor neighbor-id filter-list

Description Filter route updates to or from a neighbor based on AS path.

Syntax

```
[no] neighbor neighbor-id filter-list
AS-path-access-list {in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
AS-path-access-list	AS path list. To configure an AS path list, use the following command at the global configuration level of the CLI: **ip as-path access-list**
in | **out**	Specifies the update direction to filter: • in – Updates received from the neighbor are filtered. • out – Updates sent to the neighbor are filtered before transmission.

Default None. By default, updates are not filtered.

Mode BGP

neighbor neighbor-id maximum-prefix

Description Configure the maximum number of network prefixes that can be received in route updates from a neighbor.

NOTE: The actual maximum number of prefixes that can be configured varies depending on the platform.

Syntax

```
[no] neighbor neighbor-id maximum-prefix num [threshold]
[restart restart-interval]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
num	Maximum number of prefixes allowed. You can specify 1-1048576 for IPv4 and 1-524288 for IPv6. The default is 128. **NOTE:** The limits are platform specific.
threshold	Percentage of the allowed maximum at which a warning message is generated. You can specify 1-100. The default is 75 percent.
[restart restart-interval]	Once the BGP maximum prefix limit is reached, the BGP neighbor will be brought down and remain in the down state. To auto-restart a BGP neighbor after the configured maximum prefix limit is reached, a timer value can be specified. The BGP neighbor will then restart after the configured restart-interval.

Parameter	Description
	restart <1-1440> Range is 1 - 1440 in minutes.

Default See descriptions.

Mode BGP

Usage If the maximum is reached, the ACOS device brings down the BGP session with the peer. Configure the restart interval to reestablish the BGP session automatically at the configured time interval.

neighbor neighbor-id next-hop-self

Description Configure the ACOS device as the BGP next hop for a neighbor.

Syntax

```
[no] neighbor neighbor-id next-hop-self
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default Disabled

Mode BGP

neighbor neighbor-id override-capability

Description Override the results of capability negotiation with a neighbor.

Syntax

```
[no] neighbor neighbor-id override-capability
```

Parameter	Description
neighbor-	ID of the neighbor, which can be one of the following

Parameter	Description
id	types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default Disabled

Mode BGP

neighbor neighbor-id passive

Description Do not initiate a TCP connection with the specified neighbor, but allow the neighbor to initiate a TCP connection with the ACOS device. Once the connection is up, BGP will work over the connection.

Syntax

```
[no] neighbor neighbor-id passive
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default Disabled

Mode BGP

neighbor neighbor-id password

Description Enables MD5 authentication for sessions with a BGP neighbor.

Syntax

```
[no] neighbor neighbor-id password encrypted string
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
string	The string can be up to 80 characters long. The string can include the printable ASCII characters, which are [0-9], [a-z], and [A-Z] and are fully defined by hexadecimal value range 0x20-0x7e. The string cannot begin with a blank space, and cannot contain any of the following special characters: `' " < > & \ / ?` The password string is encrypted when viewing the the running-config and startup-config output.

Default Disabled

Mode BGP

Usage Message Digest 5 (MD5) authentication of TCP segments (as introduced in RFC 2385), provides protection of BGP sessions via the TCP MD5 Signature Option. This feature is enabled on a per-neighbor basis for the individual BGP peer configuration, and a password is required. The password must be the same on the ACOS device and on the peer (BGP neighbor).

NOTE: The **`neighbor neighbor-id password`** command is not supported in FIPS mode.

Example The following command enables MD5 for the connection with eBGP neighbor 10.10.10.22:

```
ACOS(config)# router bgp 123
ACOS(config-bgp:123)# neighbor 10.10.10.22 remote-as 456
ACOS(config-bgp:123)# neighbor 10.10.10.22 password
1234567890abcde
```

neighbor neighbor-id peer-group

Description Adds the ACOS device to a BGP peer group.

Syntax

```
[no] neighbor neighbor-id peer-group group-name
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
group-name	Name of the peer group.

Default None

Mode BGP

NOTE:

The following options are not supported for the BGP peer-group since the ACOS 6.0.0 release:

- `neighbor neighbor-id capability-orf`
- `neighbor neighbor-id default-originate`
- `neighbor neighbor-id disallow-infinite-holdtime`
- `neighbor neighbor-id distribute-list`
- `neighbor neighbor-id filter-list`
- `neighbor neighbor-id next-hop-self`
- `neighbor neighbor-id prefix-list`
- `neighbor neighbor-id send-community`
- `neighbor neighbor-id unsuppress-map`

neighbor neighbor-id prefix-list

Description Use a prefix list to filter route updates to or from a neighbor.

Syntax

```
[no] neighbor neighbor-id prefix-list list-name {in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
list-name	Name of the prefix list.
in | **out**	Specifies the update direction to filter: • in – Updates received from the neighbor are filtered. • out – Updates sent to the neighbor are filtered before transmission.

Default By default, updates are not filtered.

Mode BGP

Usage Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The ACOS device begins the search at the top of the prefix list, with rule sequence number 1. Once a match or deny occurs, the ACOS device does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top.

The neighbor distribute-list command is an alternative to the neighbor prefix-list command. Only one of these commands can be used for filtering to the same neighbor in any direction.

neighbor neighbor-id remote-as

Description Configure an internal or external BGP (iBGP or eBGP) TCP session with another router.

Syntax

```
[no] neighbor neighbor-id remote-as AS_num
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
AS_num	Neighbor's AS number.

NOTE: AS number 23456 is a reserved 2-octet AS number. An old BGP speaker (2-byte implementation) should be configured with 23456 as its remote AS number while peering with a non-mappable new BGP speaker (4-byte implementation).

Default None

Mode BGP

neighbor neighbor-id remove-private-as

Description Remove the private AS number from outbound updates.

Syntax

```
[no] neighbor neighbor-id remove-private-as
```

Parameter	Description
neighbor-	ID of the neighbor, which can be one of the following

Parameter	Description
id	types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default Disabled

Mode BGP

neighbor neighbor-id route-map

Description Apply a route map to incoming or outgoing routes.

Syntax `[no] neighbor neighbor-id route-map map-name {in | out}`

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
map-name	Name of the route map.
in | **out**	Specifies the traffic direction to which to apply the route map: • in – The route map is applied to routes received from the neighbor. • out – The route map is applied to routes sent to the neighbor.

Default None

Mode BGP

neighbor neighbor-id send-community

Description Sends community attributes to a neighbor.

Syntax

```
[no] neighbor neighbor-id send-community
[all | both | none | standard | extended | large]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
all	Sends all three community attributes such as Standard, Extended, and Large.
both	Sends both standard and extended community attributes.
none	Disables community attributes from being sent.
standard	Sends only standard community attributes.
extended	Sends only extended community attributes.
large	Sends only large community attributes.

Default By default, both standard and extended community attributes are sent to a neighbor.

Mode BGP

Usage The community attribute groups destinations in a certain community and applies routing decisions according to those communities. Upon receiving community attributes, the ACOS device re-announces them to the neighbor.

To prevent community attributes from being re-announced to the neighbor, use the “no” form of this command.

neighbor neighbor-id shutdown

Description Disable a neighbor.

Syntax

```
[no] neighbor neighbor-id shutdown
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default None

Mode BGP

Usage This command shuts down any active session for the specified neighbor and clears all related routing data.

neighbor neighbor-id soft-reconfiguration

Description Configure the ACOS device to begin storing updates, without any consideration of the applied route policy.

Syntax

```
[no] neighbor neighbor-id soft-reconfiguration inbound
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default Disabled

Mode BGP

Usage Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration can be used as an alternative to BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. When a soft reset (inbound) is performed on the neighbor, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

neighbor neighbor-id strict-capability-match

Description Close the BGP connection to a neighbor if a capability value does not completely match the value on the ACOS device.

Syntax

```
[no] neighbor neighbor-id strict-capability-match
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.

Default Enabled

Mode BGP

neighbor neighbor-id timers

Description Configure the timers for a neighbor.

Syntax

```
[no] neighbor neighbor-id timers
{interval holdtime | connect seconds}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address.

Parameter	Description
	• IPv6 address. • Name of a peer group.
interval	Amount of time in seconds between transmission of keepalive messages to the neighbor. You can specify 0-65535 seconds. The default interval is 30 seconds.
holdtime	maximum amount of time in seconds the ACOS device will wait for a keepalive message from the neighbor before declaring the neighbor dead. You can specify 0-65535 seconds. The default is 90 seconds.
seconds	Connect timer. You can specify 0-65535 seconds. In ACTIVE state, the BGP router (ACOS device) will accept an incoming connection request from the peer before the connect time expires. The default connect time is 0.

Default See descriptions.

Mode BGP

neighbor neighbor-id unsuppress-map

Description Selectively leak more-specific routes to a neighbor.

Syntax

```
[no] neighbor neighbor-id unsuppress-map map-name
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address.

Parameter	Description
	• Name of a peer group.
map-name	Name of the route map used to select routes to be unsuppressed.

Default Disabled

Mode BGP

Usage When the aggregate-address command is used with the **summary-only** option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the **unsuppress-map** command to selectively leak more-specific routes to a particular neighbor.

neighbor neighbor-id update-source

Description Allows BGP sessions to use specific source IP address or interface for TCP connections with a neighbor.

Syntax

```
[no] neighbor neighbor-id update-source source
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
source	Source IP address or interface name. **NOTE:** It is highly recommended to specify an IP address instead of an interface name. When multiple IP addresses are configured at one interface, ACOS will choose the lowest IP address as source IP address.

Default IP address of the outgoing interface to the neighbor.

Mode BGP

neighbor neighbor-id weight

Description Assign a weight value to routes learned from a neighbor.

Syntax

```
[no] neighbor neighbor-id weight num
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
num	Weight value assigned to routes learned from the neighbor. You can specify 0-65535.

Default Default weight: 0 (zero)

Mode BGP

Usage Use this command to specify a weight value, per address-family, to all routes learned from a neighbor. The route with the highest weight gets preference when the same prefix is learned from more than one peer.

Unlike the **local-preference** attribute, the **weight** attribute is relevant only to the local router.

The weights assigned using the **set weight** command override the weights assigned using this command.

When the weight is set for a peer group, all members of the peer group will have the same weight. The command can also be used to assign a different weight to a particular peer-group member. When a separately configured weight of the peer-group member is unconfigured, its weight will be reset to its peer group's weight.

neighbor <ip-addr | ipv6-addr> capability graceful-restart

Description Configure the BGP peer GR helper mode at each address family.

Syntax `[no] neighbor <ip-addr | ipv6-addr> capability graceful-restart`

Default Disabled

Mode BGP

network

Description Specify the networks to be advertised by the ACOS device's BGP routing process.

Syntax

```
[no] network {ipaddr/mask-length | ipaddr [mask network-mask]}
[backdoor]
[community community-list]
[route-map map-name]
```

Parameter	Description
ipaddr **/** *mask-length* | *ipaddr*	IPv4 Network address and mask. **NOTE:** If you are using this command under the address-family configuration level, you can only specify an IPv6 address and mask length: ***ipv6addr/****mask-length*
backdoor	Specify a backdoor BGP route.
community *community-list*	Match the specified BGP community list.
route-map *map-name*	Route map used to set or modify a value.

Default None

Mode BGP

Usage A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

nexthop

Description Configures global IPv6 address as the preferred next hop.

Syntax

```
[no] network prefer-global
```

Parameter	Description
prefer-global	Prefers a global IPv6 address as next hop address when both a global IPv6 address and an IPv6 link-local address are received for the route.

Mode BGP

Usage By default, ACOS installs the IPv6 link-local address into the Routing Information Base (RIB) and Forwarding Information base (FIB) as the forwarding next hop when both a global IPv6 address and an IPv6 link-local address are received for the route. Enabling this command changes the default behavior and allows the system to prefer the global IPv6 address as the next hop instead of the link-local address when both are present.

Limitation This is applicable only to the IPv6 address family.

Example The following commands configure global IPv6 address as the preferred next hop address:

```
ACOS(config)#router bgp 100
ACOS(config-bgp:100)#bgp router-id 100.100.100.100
ACOS(config-bgp:100)#neighbor 3340::197 remote-as 197
ACOS(config-bgp:100)#address-family ipv6
ACOS(config-bgp:100-ipv6)#nexthop prefer-global
ACOS(config-bgp:100-ipv6)#neighbor 3340::197 activate
```

redistribute

Description Redistribute route information from other sources into BGP.

Syntax

```
[no] redistribute
{
connected [route-map map-name] |
floating-ip [route-map map-name] |
ip-nat [route-map map-name] |
ip-nat-list [route-map map-name] |
isis [route-map map-name] |
```

```
lw4o6 [options] |
nat64 [route-map map-name] |
ospf [route-map map-name] |
public-ip |
rip [route-map map-name] |
static [route-map map-name] |
vip
  [only-flagged [route-map map-name] |
   only-not-flagged [route-map map-name] |
   [route-map map-name]]
}
```

Parameter	Description
connected [**route-map** *map-name*]	Redistributes route information for directly connected networks into BGP. The **route-map** option specifies the name of a configured route map.
floating-ip [**route-map** *map-name*]	Redistributes route information for floating IP addresses into BGP. The **route-map** option specifies the name of a configured route map.
ip-nat [**route-map** *map-name*]	Redistributes routes into BGP for reaching translated NAT addresses allocated from a pool. The **route-map** option specifies the name of a configured route map.
ip-nat-list [**route-map** *map-name*]	Redistributes routes into BGP for reaching translated NAT addresses allocated from a range list. The **route-map** option specifies the name of a configured route map.
isis [**route-map** *map-name*]	Redistributes route information from Intermediate System to Intermediate System (IS-IS) into BGP. The **route-map** option specifies the name of a configured route map.
lw406 [*options*]	Redistributes routes into BGP for Lightweight 4over6. (This is an IPv6 Migration feature.)
nat64 [**route-map** *map-name*]	Redistributes routes into BGP for Nat64. The **route-map** option specifies the name of a configured route map. **NOTE:** This option is only available for the **redistribute** command under the address-family configuration level.

Parameter	Description
ospf [**route-map** *map-name*]	Redistributes route information from Open Shortest Path First (OSPF) into BGP. The **route-map** option specifies the name of a configured route map.
public-ip	Redistributes public IP addresses into the BGP routing table, thereby advertising all explicitly configured public IPs via BGP. The **scaleout user-group-assignment-template** command divides the specified public IP prefixes into subnets, and these explicitly configured subnets can be advertised via BGP using this command.
static [**route-map** *map-name*]	Redistributes routes into BGP for reaching networks through static routes. The **route-map** option specifies the name of a configured route map.
vip [**only-flagged** [**route-map** *map-name*] | **only-not-flagged** [**route-map** *map-name*] | [**route-map** *map-name*]]	Redistributes routes into BGP for reaching virtual server IP addresses. To control which VIPs are redistributed, use one of the following options: • **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used. • **only-not-flagged** – Redistributes all VIPs except those on which the **redistribution-flagged** command is used. • **route-map** *map-name* -Name of a configured route map.

Default None

Mode BGP

synchronization

Description Enable IGP synchronization of iBGP learned routes.

Syntax

```
[no] synchronization
```

Default Disabled

Mode BGP

Usage Enable synchronization if the ACOS device should not advertise routes learned from iBGP neighbors, unless those routes also are present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an AS do not speak BGP and the AS is a transit for other ASs.

timers

Description Configure the BGP keepalive and holdtime timer values.

Syntax

```
[no] timers bgp interval holdtime
```

Parameter	Description
interval	Specifies the amount of time between transmission of keepalive messages to neighbors. You can specify 0-65535 seconds.
holdtime	Specifies the maximum amount of time the ACOS device will wait for a keepalive message from a neighbor before declaring the neighbor dead. You can specify 0-65535 seconds.

Default The default interval is 30 seconds. The default holdtime is 90 seconds.

Mode BGP

router bgp

To enable BGP on the ACOS device:

Enable the protocol and specify the Autonomous System (AS) number, using the following command at the global configuration level of the CLI:

```
router bgp AS-num
```

The AS-num specifies the Autonomous System Number (ASN), which can be 1-4294967295. The ACOS device supports configuration of one local AS.

Specify the ACOS device's BGP router ID:

```
bgp router-id ipaddr
```

NOTE: It is strongly recommended to manually set a unique BGP router ID for each BGP instance within the ACOS device's partitions.

Specify each of the ACOS device's neighbor (peer) BGP routers:

```
neighbor neighbor-id remote-as AS-num
```

This is the minimum required configuration. Additional configuration may be required depending on your deployment.

NOTE: It is recommended to set a fixed router-ID for all dynamic routing protocols you plan to use on the ACOS device, to prevent router ID changes caused by VRRP-A failover. If you do not explicitly configure the ACOS device's BGP router ID, BGP sessions may become reset whenever there is an interface state change.

bgp extended-asn-cap

Description Enables the ACOS device to send 4-octet BGP Autonomous System Number (ASN) capabilities.

Syntax

```
[no] bgp extended-asn-cap [asdot | asdot-plus]
```

Parameter	Description
asdot	Enables the Asdot notation. In the Asdot notation, an AS number less than 65536 is denoted as asplain that is as a decimal number and an AS number equal to or greater than 65536 is denoted as asdot+ that is two 16-bit decimal numbers joined by a dot: <high order number>.<low order number>. An AS number less than or equal to 65536 is denoted as a low order number and the high order value is set to 0. An AS number higher than 65537 is denoted starting from 1.0. For example, an AS number 65526 is denoted as the string "65526" and an AS number 65546 is represented as the string "1.10". **NOTE:** The `extended-asn-cap` must be turned ON.
asdot-plus	Enables the Asdot+ notation. In the Asdot+ notation, an AS number is denoted as two 16-bit decimal numbers joined by a dot: <high order number>.<low order number>. An AS number less than or equal to 65536 is denoted as low order number and the high order value is set to 0. An AS number higher than 65537 is denoted starting from 1.0. For example, an AS number 65526 is denoted as the string "0.65526" and an AS number 65546 is denoted as the string "1.10". **NOTE:** The `extended-asn-cap` must be turned ON.

Default `asdot` and `asdot-plus` are disabled by default.
To view the BGP connections to neighbors - See show ip bgp .
To view the summary of BGP neighbor status - See show [ip] bgp summary.
To view the information about BGP neighbors - See show [ip] bgp neighbors.

Mode Configuration mode

bgp nexthop-trigger

Description Configure BGP nexthop tracking.

Syntax

```
[no] bgp nexthop-trigger {delay seconds | enable}
```

Parameter	Description
seconds	Specifies the how long BGP waits before walking the full BGP table to determine which prefixes are affected by the nexthop changes, after receiving a trigger about nexthop changes. You can specify 1-100 seconds.
enable	Enables nexthop tracking.

Default BGP nexthop tracking is disabled by default. When you enable it, the default delay is 5 seconds.

Mode Configuration mode

trunk-stats

Description Enables the generation of statistics for trunk interfaces. It is available only in the shared partition.

Syntax

```
[no] trunk-stats enable
```

Mode Configuration mode

Example The following command enables statistics generation for the trunk interface:

```
ACOS(config)# trunk-stats enable
```

virtual-wire

virtual-wire <number>

Description Connects two virtual wire endpoints in the virtual wire. The endpoint type can be ethernet, trunk and virtual-wire-ethernet-group.

- Two endpoints must be added at a time.
- The virtual wire endpoints MTU must be the same. However, to add the ethernet interface as a member of the group, then all the members need to have the same MTU and cannot be configured as the virtual wire interface by other modules beforehand.

Syntax

```
[no] virtual-wire number
[ethernet | trunk | virtual-wire-ethernet-group]
```

Parameter	Description
ethernet	Use ethernet as virtual wire endpoint.
trunk	Use trunk as virtual wire endpoint.
virtual-wire-ethernet-group	Use virtual-wire-ethernet-group as virtual wire endpoint.

Default None

Mode Interface

Example The following command enables virtual wire with trunk endpoint:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# virtual-wire
ACOS(config-if:ethernet:1)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# virtual-wire
ACOS(config-if:ethernet:2)# interface ethernet 3
ACOS(config-if:ethernet:3)# enable
ACOS(config-if:ethernet:3)# virtual-wire
ACOS(config-if:ethernet:3)# trunk-group 10 lacp
ACOS(config-if:ethernet:3)# exit
ACOS(config)# interface trunk 10
ACOS(config-if:trunk:10)# virtual-wire
ACOS(config-if:trunk:10)# virtual-wire 1
ACOS(config-virtual-wire:1)# ethernet 1 trunk 10
```

virtual-wire-ethernet-group

Description Set ethernet interface into a virtual-wire-ethernet-group. The virtual wire ethernet group is created with ID number only.

Syntax

```
[no] virtual-wire-ethernet-group number
ethernet number [to ethernet number]
```

Default None

Mode Interface

Example The following command enables virtual wire ethernet group:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# virtual-wire
ACOS(config-if:ethernet:1)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# virtual-wire
ACOS(config-if:ethernet:2)# interface ethernet 3
ACOS(config-if:ethernet:3)# enable
ACOS(config-if:ethernet:3)# virtual-wire
ACOS(config-if:ethernet:3)# virtual-wire-ethernet-group 1
ACOS(config-virtual-wire-ethernet-group:1)#ethernet 2 to 3
```

virtual-wire-global

Description Provides options to set the virtual wire update period and update the active VLANs. These options apply to all the virtual wires in the same L3V partition.

Syntax

```
[no] virtual-wire-global
```

This command enters the **virtual-wire-global** configuration mode where the following commands are available:

Parameter	Description
vlan-update-period <*period*>	Specify this option to configure virtual wire update period. This period is the time the virtual wire needs to wait before updating the next active VLAN tag. You can specify a value from 1 to 255. The default

Parameter	Description
	value is 30 seconds. **NOTE:** • This value can be configured per partition. • You can choose a suitable value to prevent frequent updating in case the packets with inactive VLAN tags are still present in the network.
`update-active-vlan {all | l3-packet}`	Use this option to update the active VLANs. You can specify one of the following packet types: • `all` – This option forces the system to update VLAN by any kind of packet (e.g. ARP packet). • `l3-packet` – This option updates the VLAN by l3-packet. This is the default option.

Mode Configuration mode

Example The following example demonstrates **`virtual-wire-global`** usage:

```
ACOS(config)# virtual-wire-global
ACOS(config-virtual-wire-global)# vlan-update-period 60
ACOS(config-virtual-wire-global)# update-active-vlan all
```

virtual-wire-health-check

Description Configures layer 3 health check methods for virtual wire configuration.

Syntax

```
[no] virtual-wire-health-check vlan id method {ping | garp | packet-count}
```

Parameter	Description
`vlan` *id*	Specify the VLAN ID to apply the health check method so that ACOS can detect the active or standby mode of the VLAN.
`method`	Specify the method to be used for the health check

Parameter	Description
	that allows ACOS to detect the active or standby mode of VLAN. The available methods are: • ping - The 'ping' method monitors the incoming traffic on the VLAN. ACOS sends an ICMP echo request to the target IP address and checks for the response. If it does not receive a response to two consecutive echo requests, the VLAN status is marked as standby. • garp - The 'Gratuitous ARP' method monitors the GARP packets on the target address or interface for a specified interval. If GARP packets are not received within the configured interval, the VLAN status is marked as standby. • packet-count - The 'packet count' method monitors the packet rate on the virtual wire for a specified active threshold. If it falls below this threshold, the VLAN status is marked as standby.

The **ping** method command enters the ping configuration mode, where the following options are available:

Table 17 : Sub-commands in the Ping Method configuration mode

Parameter	Description
interface {ethernet *eth-id* **| trunk** *trunk-id***}**	Mandatory. Specify the output interface through which the echo request (ping) will be sent. The following interfaces can be specified: • **ethernet** *eth-id* - Specify the Ethernet

Table 17 : Sub-commands in the Ping Method configuration mode

Parameter	Description
	interface ID number. • **trunk** *trunk-id* - Specify the trunk interface ID number.
interval *num*	Specify the time interval, in seconds, between each health check entry. By default, the value is set to 3 seconds. The value can range from 1 to 180 seconds.
nexthop-ip *ipv4-address* **{nexthop-mac** *mac-address***}**	Mandatory. Specify the nexthop IPv4 address of the target device. Optionally, specify the nexthop mac address of the target device. The MAC address can be in dot-separated or colon-separated formats: `aabb.ccdd.eeff` or `AA:BB:CC:DD:EE:FF`.
source-ip *ipv4-address* **{source-mac** *mac-address***}**	Specify the source IP address to be used for the ping request. Optionally, specify the source MAC address to be used for the ping request. The mac-address can be in dot-separated or colon-separated formats: `aabb.ccdd.eeff` or `AA:BB:CC:DD:EE:FF`. **Additional Notes:** • When both the **source-ip** and **source-mac**, and the **nexthop-ip** and **nexthop-mac** are configured, ACOS will send the ping request directly using this information without inspecting the traffic. • If only part of the information (**source-ip** or **nexthop-ip**) is configured, ACOS will analyze the

Table 17 : Sub-commands in the Ping Method configuration mode

Parameter	Description
	traffic matching the virtual port to gather the necessary fields and then send the ping request.
inner-vlan *vlan-id*	Specify the inner VLAN ID for 802.1 Q-in-Q environment. The VLAN ID can be in the range of 2 to 4094.
partition-health-check	Enable the partition health check option for the ping method. If this option is configured and the health check entry is in standby status, all traffic received within the partition will be processed according to standby logic.
enable	Mandatory. Enable the health check method on the virtual wire VLAN. The health check takes effect only when this option is configured.

The **garp** method command enters the garp configuration mode, where the following options are available:

Table 18 : Sub-commands in the GARP Method configuration mode

Parameter	Description
interface {ethernet *eth-id* **| trunk** *trunk-id***}**	Mandatory. Specify the interface that will receive GARP packets when the device is in active mode. The following interfaces can be specified: • **ethernet** *eth-id* - Specify the Ethernet interface ID number. • **trunk** *trunk-id* - Specify the trunk interface ID number.
interval *num*	Specify the time interval, in seconds, between

Table 18 : Sub-commands in the GARP Method configuration mode

Parameter	Description
	each health check entry. By default, the value is set to 3 seconds. The value can range from 0 to 180 seconds. If you set the value to 0, ACOS will only detect the VLAN status by **interface** and **standby-interface** options.
nexthop-ip *ipv4-address*	Mandatory. Specify the nexthop IPv4 address of the target device.
standby-interface {ethernet *eth-id* **| trunk** *trunk-id***}**	Specify the interface that will receive GARP packets when the device is in standby mode. If ACOS receives GARP packet from the "standby-interface", the VLAN is changed to standby immediately without waiting for the configured interval. The following interfaces can be specified: • **ethernet** *eth-id* - Specify the Ethernet interface ID number. • **trunk** *trunk-id* - Specify the trunk interface ID number.
partition-health-check	Enable the partition health check option for the GARP method. If this option is configured and the health check entry is in standby status, all traffic received within the partition will be processed according to standby logic.
enable	Enable the health check method on the virtual wire VLAN. The health check takes effect only when this is configured.

The **packet-count** method command enters the packet-count configuration mode, where the following options are available:

Table 19 : Sub-commands in the Packet Count Method configuration mode

Parameter	Description
active-threshold *num*	Mandatory. Specify the expected packet rate (in packets per second) for active mode. If the packet rate on the target interface falls below this threshold, the VLAN status is marked as standby. If the packet rate is above this threshold, the VLAN status is marked as active.
interface {ethernet *eth-id* **| trunk** *trunk-id***}**	Mandatory. Specify the target interface to monitor the packet rate. The following interfaces can be specified: • **ethernet** *eth-id* - Specify the Ethernet interface ID number. • **trunk** *trunk-id* - Specify the trunk interface ID number.
interval *num*	Specify the time interval, in seconds, between each health check entry. This interval determines how frequently ACOS checks the packet rate on the specified interface. By default, the value is set to 3 seconds. The value can range from 1 to 180 seconds.
l3-packet	Enable this option if you want to count only the Layer 3 packets. ACOS only counts the packet rate for IPv4 and IPv6 packets, excluding other types of packets from the count.
inner-vlan *vlan-id*	Specify the inner VLAN ID for the 802.1Q-in-Q environment. The VLAN ID can be in the range of 2 to 4094.

Table 19 : Sub-commands in the Packet Count Method configuration mode

Parameter	Description
	ACOS only counts the packet rate for packets with the specified inner VLAN ID.
`partition-health-check`	Enable the partition health check option for the packet count method. If this option is configured and the health check entry is in standby status, all traffic received within the partition will be processed according to standby logic.
`enable`	Enable the health check method on the virtual wire VLAN. The health check takes effect only when this is configured.

Mode Configuration mode

Usage ACOS provides layer 3 health monitoring support for virtual wire and virtual wire with SSLi (IP-less), which operates transparently in high-availability deployments. In these deployments, two firewall devices manage the active and standby paths during failover scenarios.

Layer 3 health checks can be configured on the VLAN that needs monitoring.

The health check enables ACOS to determine whether the VLAN is in active or standby mode by using the ping, gratuitous ARP (GARP), and packet count methods. Additionally, the health check prevents ACOS from sending the packets to the ACOS standby devices, thus avoiding network disturbances. The health check works on ACOS device only.

Only one method can be mapped with a VLAN. It is recommended not to change the health check method of the configured VLAN at runtime.

For more information, see Network Configuration Guide and SSL Insight (SSLi) Configuration Guide.

Example The following example demonstrates **virtual-wire-health-check** with ping method:

```
ACOS(config)# virtual-wire-health-check vlan 10 method ping
ACOS(config-virtual-wire-health-check:10)# interface ethernet
4
ACOS(config-virtual-wire-health-check:10)# interval 5
ACOS(config-virtual-wire-health-check:10)# nexthop-ip
10.10.10.3
ACOS(config-virtual-wire-health-check:10)# enable
```

Example The following example demonstrates **virtual-wire-health-check** with ping method, where source IP, nexthop IP, and MAC addresses are also configured:

```
ACOS(config)# virtual-wire-health-check vlan 10 method ping
ACOS(config-virtual-wire-health-check:10)# interface ethernet
4
ACOS(config-virtual-wire-health-check:10)# interval 5
ACOS(config-virtual-wire-health-check:10)# nexthop-ip
10.10.10.3 nexthop-mac 000c.2991.3b76
ACOS(config-virtual-wire-health-check:10)# source-ip
10.10.10.123 source-mac 1122.3344.5566
ACOS(config-virtual-wire-health-check:10)# enable
```

Example The following example demonstrates **virtual-wire-health-check** with garp method:

```
ACOS(config)# virtual-wire-health-check vlan 10 method garp
ACOS(config-virtual-wire-health-check:10)# interface ethernet
4
ACOS(config-virtual-wire-health-check:10)# interval 5
ACOS(config-virtual-wire-health-check:10)# nexthop-ip
10.10.10.3
ACOS(config-virtual-wire-health-check:10)# standby-interface
ethernet 5
ACOS(config-virtual-wire-health-check:10)# enable
```

Example The following example demonstrates **virtual-wire-health-check** with packet-count method:

```
ACOS(config)# virtual-wire-health-check vlan 10 method packet-count
ACOS(config-virtual-wire-health-check:10)# interface ethernet 4
ACOS(config-virtual-wire-health-check:10)# interval 5
ACOS(config-virtual-wire-health-check:10)# active-threshold 5
ACOS(config-virtual-wire-health-check:10)# enable
```

virtual-wire-vlan-pair

Description Configure and map the active and passive VLAN tags to track the active VLAN pair in the network environment for virtual-wire sessions.

Prerequisite

- interface
- vlan

Syntax

```
[no] virtual-wire-vlan-pair pair-id [vlan first-vlan-id vlan second-vlan-id]
```

This command enters the **virtual-wire-vlan-pair** configuration mode, where the following commands are available:

Parameter	Description
pair-id	Specify the virtual-wire pair ID. The value can be between 1 to 16.
vlan first-vlan-id	Specify the first VLAN ID that will be in active state. The value can be between 2 to 4094.
vlan second-vlan-id	Specify the second VLAN ID that will be in active state. The value can be between 2 to 4094.

Mode Global configuration

Usage This command applies to the virtual wire with SSLi IP-less deployment, where firewall networking devices are used for upstream and

downstream traffic. The firewall devices govern the active standby paths in failover scenarios.

The **virtual-wire-vlan-pair** facilitates ACOS to know that only two VLAN tags can be active at the same time for the virtual wire session. These two VLAN pairs are then configured in the **virtual-wire-vlan-set**. This helps ACOS to track and update the active VLAN pair in the network and forward the traffic to the active server.

Additionally, ACOS matches the packet to the correct virtual wire session even if the forward and reverse traffic uses a different VLAN or the VLAN is changed due to firewall failover. This capability ensures that traffic is distributed seamlessly during failover scenarios.

For detailed implementation details, see *Network Configuration Guide* and *SSL Insight Configuration Guide*.

Limitation

- This feature is only supported for slow paths.
- Making changes to **virtual-wire-vlan-pair** or **virtual-wire-vlan-pair-set** configurations in production may cause some virtual wire sessions to use the incorrect active VLAN.

Example

The following example demonstrates **virtual-wire-vlan-pair** usage. Here, the two VLAN pairs **1** and **2** are configured. Active VLAN 2001 and 2003, and passive VLAN 2002 and 2004.

```
ACOS(config)# virtual-wire-vlan-pair 1
ACOS(config-virtual-wire-vlan-pair:1)# vlan 2001 vlan 2003
ACOS(config-virtual-wire-vlan-pair:1)# exit
ACOS(config)# virtual-wire-vlan-pair 2
ACOS(config-virtual-wire-vlan-pair:2)# vlan 2002 vlan 2004
ACOS(config-virtual-wire-vlan-pair:2)# exit
```

The active VLAN is updated in the order specified in the virtual wire VLAN pair. For example, if a virtual-wire session used active VLAN **2001**, and the active VLAN for **virtual-wire-vlan-pair 2** needs to be updated, then ACOS updates VLAN to **2002** because 2001 and 2002 are the first VLAN in the pairs.

Related Commands:

- virtual-wire-vlan-pair-set

virtual-wire-vlan-pair-set

Description Configure the virtual wire VLAN pair set and map the two virtual wire VLAN pairs to track active VLAN pairs in the network environment for virtual-wire sessions.

Prerequisite

- interface
- vlan
- virtual-wire-vlan-pair

Syntax

```
[no] virtual-wire-vlan-set set-id [virtual-wire-vlan-pair
active-pair-id virtual-wire-vlan-pair passive-pair-id]
```

This command enters the **virtual-wire-vlan-set** configuration mode, where the following commands are available:

Parameter	Description
set-id	Specify the virtual-wire pair set ID. The value can be between 1 to 8.
virtual-wire-vlan-pair active-pair-id	Specify the active virtual-wire-vlan-pair ID. The value can be between 1 to 16.
virtual-wire-vlan-pair passive-pair-id	Specify the passive virtual-wire-vlan-pair ID. The value can be between 1 to 16.

Mode Global configuration

Usage See virtual-wire-vlan-pair.

Limitation

- This feature is only supported for slow paths.
- Making changes to **virtual-wire-vlan-pair** or **virtual-wire-vlan-pair-set** configurations in production may cause some virtual wire sessions to use the incorrect active VLAN.

Example The following example demonstrates **virtual-wire-vlan-pair-set** usage. Here, the two VLAN pair IDs are mapped with the virtual wire VLAN set.

```
ACOS(config)# virtual-wire-vlan-set 1
ACOS(config-virtual-wire-vlan-pair-set:1)# virtual-wire-vlan-pair 1
ACOS(config-virtual-wire-vlan-pair-set:1)# virtual-wire-vlan-pair 2
ACOS(config-virtual-wire-vlan-pair-set:1)# exit
```

vlan

Description Configure a virtual LAN (VLAN). This command changes the CLI to the configuration level for the VLAN.

Syntax

```
[no] vlan vlan-id
```

Replace *vlan-id* with the ID of the VLAN (2-4094).

If the ACOS device is a member of an aVCS virtual chassis, specify the *vlan-id* as follows:

DeviceID/*vlan-id*

Default VLAN 1 is configured by default. All Ethernet data ports are members of VLAN 1 by default.

Mode Configuration mode

Usage You can add or remove ports in VLAN 1 but you cannot delete VLAN 1 itself.

Example The following command adds VLAN 69 and enters the configuration level for that VLAN:

```
ACOS(config)# vlan 69
ACOS(config-vlan:69)#
```

Example You cannot have duplicate VLANs configured across partitions. In this example, VLAN 10 is configured in the shared partition:

```
ACOS(config)# vlan 10
```

```
ACOS(config-vlan:10)# exit
ACOS(config)#
```

If you attempt to configure VLAN 10 in an L3V partition, you will receive an error message:

```
ACOS(config)# active-partition p2
Current active partition: p2
ACOS[p2]# configure
ACOS[p2](config)# vlan 10
This VLAN or Port is owned by another partition.
```

name

Description Assign a name to the VLAN.

Syntax

```
[no] name string
```

Replace *string* with the name for the VLAN, 1-63 characters.

Default The default name for VLAN 1 is “DEFAULT VLAN”. For other VLANs, if a name is not configured, “None” appears in place of the name.

Mode VLAN

Example The following commands assign the name “Test100” to VLAN 100 and show the result:

```
ACOS(config)# vlan 100
ACOS(config-vlan:100)# name Test100
ACOS(config-vlan:100)# show vlan
Total VLANs: 3
VLAN 1, Name [DEFAULT VLAN]:
  Untagged Ports:    3   4   5   6   7   9  10
    Tagged Ports:   None

VLAN 100, Name [Test100]:
  Untagged Ports:    1
    Tagged Ports:   None
 Router Interface: ve 1

VLAN 200, Name [None]:
  Untagged Ports:    2
```

```
   Tagged Ports:   None
Router Interface: ve 2
```

router-interface

Description Add a virtual Ethernet (VE) router interface to the VLAN. A VE is required in order to configure an IP address on a VLAN.

Syntax

```
[no] router-interface ve ve-num
```

Replace *ve-num* with the VE number, 2-4094. The VE number must be the same as the VLAN number.

Default By default, a VLAN does not have a VE.

Mode VLAN

Usage This command is valid only on ACOS devices deployed in route mode.

The VE interface on a VLAN must have the same number as the VLAN. For example, in VLAN 69, the VE number also must be 69.

MAC Address Assignment

The MAC addresses used by the ACOS device's physical Ethernet data ports also are used for VEs. (See the "system ve-mac-scheme" command in the *Command Line Interface Reference*.)

Example The following command configures VE 4 on VLAN 4:

```
ACOS(config)# vlan 4
ACOS(config-vlan:4)# router-interface ve 4
```

shared-vlan

Description Enable the shared management VLAN functionality for the VLAN.

Syntax

```
[no] shared-vlan
```

Default Disabled

Mode VLAN

Example The following command configures VLAN 100 as a shared VLAN:

```
ACOS(config)# vlan 100
ACOS(config-vlan:100)# shared-vlan
```

tagged

Description Add tagged ports to a VLAN. A tagged port can be a member of more than one VLAN. An untagged port can be a member of only a single VLAN.

Syntax

```
[no] tagged
{ethernet port-num [to port-num] | trunk trunk-num [to trunk-num]}
```

Parameter	Description
port-num	Add the specified tagged ethernet port to the VLAN. To add a range of ports, use the **to** *port-num* option.
trunk-num	Add the specified tagged trunk to the VLAN. To add a range of trunks, use the **to** *trunk-num* option.

Default A VLAN has no ports by default.

Mode VLAN

Usage A port can be a tagged member of a maximum of 128 VLANs.

Example The following command adds ports 4 and 5 to VLAN 4 as tagged ports:

```
ACOS(config)# vlan 4
ACOS(config-vlan:4)# tagged ethernet 4 to 5
```

traffic-distribution-mode

Description Distributes the traffic to a specific destination based on the mode selected.

Syntax

```
[no] traffic-distribution-mode [ sip | dip | l3-lookup |
primary | blade | l4-src-port | l4-dst-port ]
```

Command	Description
sip	Distribute the traffic evenly to the Multi-PUs (PU1 and PU2) based on the source IP address.
dip	Distribute the traffic evenly to the Multi-PUs (PU1 and PU2) based on the destination IP address.
l3-lookup	Specify this distribution mode for a DMZ-facing interface to distribute traffic evenly across Multi-PUs based on the result of an L3 lookup, populated via class-list of client IP addresses. The class list of client IP addresses can be configured using the fw client class-list command.
primary	Distribute the traffic to the primary (master) unit.
blade	Distribute the traffic to the secondary (blade) unit.
l4-src-port	Distribute the traffic to the Multi-PUs based on the layer 4 source port.
l4-dst-port	Distributes the traffic to the Multi-PUs based on the layer 4 destination port.

Mode VLAN or Interface

Usage This command is used to define the traffic distribution mode.

Example The following command sets the traffic distribution mode as **sip/dip** in VLAN:

```
ACOS(config)# vlan 90
ACOS(config-vlan:90)# traffic-distribution-mode sip
ACOS(config)# vlan 91
ACOS(config-vlan:90)# traffic-distribution-mode dip
```

Example The following command sets the traffic distribution mode as **l3-lookup** in VLAN:

```
ACOS(config)# vlan 211
ACOS(config-vlan:211)# tagged ethernet 13
ACOS(config-vlan:211)# router-interface ve 211
ACOS(config-vlan:211)# traffic-distribution-mode l3-lookup
```

Example The following command sets the traffic distribution mode as **sip or dip** in the Interface ethernet:

```
ACOS(config)# interface ethernet 6
ACOS(config-if:ethernet:6)# enable
ACOS[ssli_in](config-if:ethernet:6)# traffic-distribution-mode
dip
ACOS(config)# interface ethernet 7
ACOS(config-if:ethernet:7)# enable
ACOS(config-if:ethernet:7)# traffic-distribution-mode sip
```

Related Commands:

- vlan
- interface
- system chassis-port-split
- odd-even-nat-enable

untagged

Description Add untagged ports to a VLAN. An untagged port can be a member of only a single VLAN.

Syntax

```
[no] untagged
{
ethernet port-num [to port-num] |
lif lif-num |
trunk trunk-num [to trunk-num] |
}
```

Parameter	Description
port-num	Add the specified untagged ethernet port to the VLAN. To add a range of ports, use the **to** *port-num* option.
lif-num	Add the specified logical interface to the VLAN.
trunk-num	Add the specified untagged trunk to the VLAN. To add a range of trunks, use the **to** *trunk-num* option.

Default VLAN 1 contains all ports by default. New VLANs do not contain any ports by default.

Mode VLAN

Example The following command adds port 6 and ports 8-10 to VLAN 4 as an untagged ports:

```
ACOS(config)# vlan 4
ACOS(config-vlan:4)# untagged ethernet 6
ACOS(config-vlan:4)# untagged ethernet 8 to 10
```

untagged lif

Description Configures an untagged Layer 2 logical tunnel interface (LIF) under a VLAN.

NOTE: Only one untagged logical tunnel interface is supported under a VLAN. Having more than one logical tunnel interface in the same VLAN will result in traffic being “switched” between VNIs which is not supported.

Syntax

```
untagged lif lif-num
```

Replace *lif-num* with the number of the logical interface.

Default N/A

Mode VLAN configuration mode.

Example Configure an untagged logical interface number 2 under VLAN 10.

```
ACOS(config)# vlan 10
ACOS(config-vlan:10)# untagged lif 2
```

Related Commands:

- interface lif

Show Commands

clear [ip] bgp {* | AS-num}

Description Reset the BGP connection to all neighbors or a specific neighbor.

Syntax

```
clear [ip] bgp {* | AS-num}
[in [prefix-filter] | out | soft [in | out]]
```

Parameter	Description
in [**prefix-filter**]	Clears incoming advertised routes. The **prefix-filter** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.
out	Clears outgoing advertised routes.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. **in** – Requests route updates from the specified neighbor. **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp external

Description Reset the BGP connection to external neighbors.

Syntax

```
clear [ip] bgp external
[in [prefix-filter] | out | soft [in | out]]
```

Parameter	Description
in [**prefix-**	Clears incoming advertised routes. The **prefix-**

Parameter	Description
filter]	**filter** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.
out	Clears outgoing advertised routes.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. • **in** – Requests route updates from the specified neighbor. • **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp ipv4

Description Reset dampened routes or route-flap statistics counters and history for IPv4.

Syntax

```
clear [ip] bgp ipv4 {multicast | unicast}
{dampening | flap-statistics}
[ipv4addr | ipv4addr/mask-length]
```

Parameter	Description
dampening	Resets dampened routes.
flap-statistics	Resets route-flap statistics and history.
ipv4addr | *ipv4addr* **/***mask-length*	Resets dampened routes or route-flap statistics and history only for the specified IPv4 prefix.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp ipv4addr

Description Reset the BGP connection for a specific IPv4 neighbor.

Syntax

```
clear [ip] bgp ipv4addr
[in [prefix-filter] | out | soft [in | out]]
```

Parameter	Description
in [**prefix-filter**]	Clears incoming advertised routes. The **prefix-filter** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.
out	Clears outgoing advertised routes.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. **in** – Requests route updates from the specified neighbor. **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp ipv6

Description Reset dampened routes or route-flap statistics counters and history for IPv6.

Syntax

```
clear [ip] bgp ipv6 {
unicast {dampening [network] | flap-statistics  network} |
{external | peer-group  group-name | * | as-num | ipv4addr |
ipv6addr}
  [in [prefix-filter] | out | soft [in | out]]
}
```

Parameter	Description
unicast	Resets unicast routes.
external	Clear all external peers.

Parameter	Description
	NOTE: This option is only available with **clear bgp ipv6**.
dampening [*network*]	Resets all IPv6 dampened routes. To reset dampened routes for an specific network, specify either an IPv6 network (for example, "2003::") or a network length (for example, "2003::/24").
flap-statistics [*network*]	Resets all IPv6 route-flap statistics and history. To reset route-flap statistics and history for a specific network, specify either an IPv6 network (for example, "2003::") or a network length (for example, "2003::/24").
peer-group	Clear all members of the specified peer group.
*	Clear all peers.
as-num	Clear all peers with the specified AS number.
ipv4-addr	Clear the specified IPv4 BGP neighbor.
ipv6-addr	Clear the specified IPv6 BGP neighbor.
in [**prefix-filter**]	Clears incoming advertised routes. The **prefix-filter** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.
out	Clears outgoing advertised routes.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. **in** – Requests route updates from the specified neighbor. **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp ipv6addr

Description Reset the BGP connection for a specific IPv6 neighbor.

Syntax

```
clear [ip] bgp ipv6addr
[in [prefix-filter] | out | soft [in | out]]
```

Parameter	Description
in [**prefix-filter**]	Clears incoming advertised routes. The **prefix-filter** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.
out	Clears outgoing advertised routes.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. **in** – Requests route updates from the specified neighbor. **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp peer-group

Description Reset the BGP connection to all members of a peer group.

Syntax

```
clear [ip] bgp peer-group group-name
[in [prefix-filter] | out | soft [in | out]]
```

Parameter	Description
group-name	Clear BGP connections to all members of the specified group.
in [**prefix-filter**]	Clears incoming advertised routes. The **prefix-filter** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.

Parameter	Description
out	Clears outgoing advertised routes.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. **in** – Requests route updates from the specified neighbor. **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp view

Description Reset the BGP connection to a specific view.

Syntax

```
clear [ip] bgp view view-name * [soft [in | out]]
```

Parameter	Description
view-name	Clear BGP connections to the specified view.
soft {**in** | **out**}	Activates routing policy changes without resetting the BGP neighbor connection. **in** – Requests route updates from the specified neighbor. **out** – Sends route updates to the specified neighbor.

Mode Privileged EXEC and all configuration levels

Related Commands:

- clear [ip] bgp {* | AS-num}

clear ip rip route

Description Clears routes from the IPv4 RIP table.

Syntax

```
clear ip rip route {ipaddr/mask-length | rip}
```

Parameter	Description
ipaddr/*mask-length*	Replace ipaddr/mask-length to clear the route to the specified network.
rip	Clears all RIP routes from the table.

Mode Privileged EXEC or any configuration level

clear ipv6 rip route

Description Clears routes from the IPv6 RIP table.

Syntax

```
clear ipv6 rip route
{ipv6addr/mask-length | rip}
```

Parameter	Description
ipv6addr/*mask-length*	Clears the route to the specified network.
rip	Clears all RIP routes from the table.

Mode Privileged EXEC or any configuration level

show [ip] bgp community

Description Display routes for communities.

Syntax

```
show [ip] bgp community [community-number]
[exact-match] [local-AS] [no-advertise] [no-export]
```

Parameter	Description
community-number	Community number, in *AA:NN* format.
exact-match	Displays only communities that exactly match.
local-AS	Displays only communities that are not sent outside the local AS.

Parameter	Description
no-advertise	Displays only communities that are not sent advertised to neighbors.
no-export	Displays only communities that are not exported to the next AS.

Mode All

show [ip] bgp community-list

Description Display routes for a specific community list.

Syntax

```
show [ip] bgp community-list list-name [exact-match]
```

Parameter	Description
list-name	Displays routes matching the specified community list.
exact-match	Displays only the routes that have exactly the same communities.

Mode All

show [ip] bgp dampening

Description Display route-flap dampening information.

Syntax

```
show [ip] bgp dampening
{dampened-paths | flap-statistics | parameters}
```

Parameter	Description
dampened-paths	Displays paths suppressed due to dampening.
flap-statistics	Displays flap statistics for routes.
parameters	Displays details for configured dampening parameters.

Mode All

show [ip] bgp filter-list

Description Display routes that match a specific filter list.

Syntax

```
show [ip] bgp filter-list list-name
```

Mode All

show [ip] bgp inconsistent-as

Description Display routes that have inconsistent AS Paths.

Syntax

```
show [ip] bgp inconsistent-as
```

Mode All

show [ip] bgp ipv4 {multicast | unicast}

Description Display BGP information for IPv4.

Syntax

```
show [ip] bgp ipv4 {multicast | unicast}
[
ipv4addr |
ipv4addr/mask-length |
community [community-number] [exact-match]
  [local-AS] [no-advertise] [no-export] |
community-list list-name [exact-match] |
dampening {dampened-paths | flap-statistics | parameters} |
filter-list list-name |
flowspec |
inconsistent-as |
labeled |
large-community |
large-community-list |
neighbors [ipv4addr | ipv6addr
  [advertised-routes | received prefix-filter | received-
routes | routes]] |
paths |
prefix-list list-name |
quote-regexp string |
regexp string [string ...] |
route-map map-name |
summary |
```

```
unicast
]
```

Parameter	Description
multicast | **unicast**	Specifies the IPv4 address family for which to display information.
ipv4addr | ipv4addr/mask-length	Network and mask information.
community [*community-number*] [*options*]	Displays routes matching the communities. Enter the community number in AA:NN format. The following options are supported: • exact-match – Displays only communities that exactly match. • local-AS – Displays only communities that are not sent outside the local AS. • no-advertise – Displays only communities that are not sent advertised to neighbors. • no-export – Displays only communities that are not exported to the next AS.
community-list *list-name* [**exact-match**]	Displays routes matching the specified community list. The **exact-match** option displays only the routes that have exactly the same communities.
dampening {*options*}	Displays route-flap dampening information. You must specify one of the following options: • dampened-paths – Displays paths suppressed due to dampening. • flap-statistics – Displays flap statistics for routes. • parameters – Displays details for configured dampening parameters.
filter-list	Displays routes that match the specified filter

Parameter	Description
list-name	list.
inconsistent-as	Displays routes that have inconsistent AS Paths.
large-community*num*	Displays routes matching the large communities. Large community number in the format XX:YY:ZZ.
large-com-munity-list *list-name*	Displays routes matching the large community-list.
neighbors [*ipv4addr* | *ipv6addr* [options]]	Displays detailed information about TCP and BGP neighbor connections. The following options are supported: • advertised-routes – Displays the routes advertised to a BGP neighbor. • received prefix-filter – Displays all received routes, both accepted and rejected. • received-routes – Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first. • routes – Displays all accepted routes learned from neighbors.
paths	Displays path information.
prefix-list *list-name*	Displays routes that match the specified prefix list.
quote-regexp *string*	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).
regexp *string* [*string* ...]	Displays routes that match the specified AS-path regular expression(s).

Parameter	Description
route-map *map-name*	Displays routes that match the specified route map.
summary	Displays a summary of BGP neighbor status.

Mode All

show [ip] bgp paths

Description Display BGP path information.

Syntax

```
show [ip] bgp paths
```

Mode All

show [ip] bgp prefix-list

Description Displays routes that match a specific prefix list.

Syntax

```
show [ip] bgp prefix-list list-name
```

Mode All

show [ip] bgp quote-regexp

Description Display routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).

Syntax

```
show [ip] bgp quote-regexp string
```

Mode All

show [ip] bgp regexp

Description Display routes that match the specified AS-path regular expression(s).

Syntax

```
show [ip] bgp regexp string [string ...]
```

Mode All

show [ip] bgp route-map

Description Display routes that match the specified route map.

Syntax

```
show [ip] bgp route-map map-name
```

Mode All

show [ip] bgp summary

Description Displays a summary of BGP neighbor status.

Syntax

```
show [ip] bgp summary
```

Mode All

Example The following example shows output for the `show [ip] bgp summary` command when the `asdot` notation is configured:

```
ACOS#show ip bgp summary
BGP router identifier 10.10.10.198, local AS number 198
BGP table version is 3
BGP advertisement is enabled
4 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS
MsgRcvd MsgSent TblVer InQ OutQ Up/Down
State/PfxRcd/PfxSent
10.10.10.197 4 197
12 15 2 0 0 00:00:55 1/ 1

Total number of neighbors 1
```

Example The following example shows output for the `show [ip] bgp summary` command when the `asdot-plus` notation is configured:

```
ACOS#show ip bgp summary
BGP router identifier 10.10.10.198, local AS number 0.198
```

```
BGP table version is 2
BGP advertisement is enabled
3 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS MsgRcvd
MsgSent TblVer InQ OutQ Up/Down State/PfxRcd/PfxSent
10.10.10.197 4 0.197
3 3 1 0 0 00:00:02 1/ 1

Total number of neighbors 1
```

show {ip | ipv6} ospf

Description Display configuration information and statistics for OSPFv2 processes or OSPFv3 processes.

Syntax

```
show ip ospf [process-id]

show ipv6 ospf [tag]
```

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, settings for all configured OSPFv2 processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, settings for all configured OSPFv3 processes are displayed.

Mode Privileged EXEC and all configuration levels

Example The following command shows information for OSPFv2 process 0:

```
ACOS#show ip ospf 0
 Routing Process "ospf 0" with ID 1.1.1.1
 Process uptime is 3 hours 12 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is
disabled
 Supports only single TOS(TOS0) routes
```

```
 Supports opaque LSA
 This router is an ASBR (injecting external routing
information)
 SPF schedule delay min 0.500 secs, SPF schedule delay max
50.0 secs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 2
 Number of LSA received 79
 Number of areas attached to this router: 1
    Area 1 (NSSA)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 2
        Number of fully adjacent virtual neighbors through
this area is 0
        Area has no authentication
        SPF algorithm last executed 02:07:40.860 ago
        SPF algorithm executed 16 times
        Number of LSA 10. Checksum 0x06b2fa
        NSSA Translator State is disabled
        Shortcutting mode: Default, S-bit consensus: ok
```

show {ip | ipv6} ospf interface

Description Display OSPF information for an interface.

Syntax

```
show {ip | ipv6} ospf interface
{ethernet portnum | lif num | loopback num | management |
  trunk num | tunnel num | ve ve-num}
```

Mode Privileged EXEC and all configuration levels

Example The following command shows OSPFv3 information for interface Ethernet 1:

```
ACOS#show ipv6 ospf interface
```

```
ethernet 1 is up, line protocol is up
  Interface ID 3
  IPv6 Prefixes
    fe80::21f:a0ff:fe04:d7e4/64 (Link-Local Address)
    1000::1/32
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 100.1.1.1, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 9.1.1.1
      Interface Address fe80::21f:a0ff:fe04:b1f0
    Backup Designated Router (ID) 100.1.1.1
      Interface Address fe80::21f:a0ff:fe04:d7e4
    Timer interval configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
      Hello due in 00:00:02
    Neighbor Count is 1, Adjacent neighbor count is 1
```

show {ip | ipv6} ospf neighbor

Description Display information about OSPF neighbors.

Syntax

```
show ip ospf neighbor
[ipaddr [detail]] |
[all] |
[detail [all]] |
[interface interface-num]]
```

Syntax

```
show ipv6 ospf [tag] neighbor
[ipaddr [detail]] |
[detail [all]] |
[interface interface-num]
```

NOTE: The all option applies only to OSPFv2.

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3

Parameter	Description
	processes are displayed.
ipaddr [**detail**]	Displays information for the specified neighbor. For detailed information, use the detail option. For summary information, omit the detail option.
all	Includes neighbors whose status is Down. Without this option, down neighbors are not included in the output.
detail [**all**]	Displays detailed information for all neighbors. To include down neighbors in the output, use the all option.
interface *ipaddr*	Displays information for neighbors reachable through the specified IP interface.

Mode Privileged EXEC and all configuration levels

Example The following command shows information for OSPFv2 neighbors:

```
ACOS#show ip ospf neighbor

OSPF process 0:
Neighbor ID    Pri    State   Dead Time Address   Interface
Instance ID
-------------------------------------------------------
9.1.1.1   1    Full/Backup    00:00:34 10.1.1.2 ethernet 1   0
```

show {ip | ipv6} ospf route

Description Display information for OSPFv2 routes.

Syntax

```
show ip ospf [process-id] route

show ipv6 ospf [tag] route
```

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2

Parameter	Description
	processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes are displayed.

Mode Privileged EXEC and all configuration levels

Example The following command shows OSPFv2 IPv4 routes and OSPFv3 IPv6 routes:

```
ACOS#show ip ospf route
IA 0.0.0.0/0 [2] via 10.0.0.1, ve 1, Area 0.0.0.1
O  1.0.4.0/24 [2] via 13.0.0.2, ve 2, Area 0.0.0.1
C  10.0.0.0/24 [1] is directly connected, ve 1, Area 0.0.0.1
O  11.0.0.0/24 [2] via 10.0.0.1, ve 1, Area 0.0.0.1

ACOS#show ipv6 ospf route
OSPFv3 Process (*null*)  Total = 1
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter
area
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
C  1000::/32                                          10
     directly connected, ethernet 1, Area 0.0.0.0
E2 9111::/32                                        10/20
     via fe80::21f:a0ff:fe04:b1f0, ethernet 1
```

show {ip | ipv6} ospf virtual-links

Description Display virtual link information.

Syntax

```
show ip ospf [process-id] virtual-links

show ipv6 ospf [tag] virtual-links
```

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes are displayed.

Mode Privileged EXEC and all configuration levels

Example The following command shows information for OSPFv2 virtual links:

```
ACOS#show ip ospf virtual-link
Virtual Link VLINK1 to router 143.0.0.143 is up
  Transit area 0.0.0.1 via interface ethernet 1
  Local address 13.0.0.2/32
  Remote address 13.0.0.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:10
Adjacency state Full

ACOS#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface eth0, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
```

show bgp ipv4 neighbors

Description Display information about IPv4 BGP neighbors.

Syntax

```
show bgp ipv4 neighbors
[ipv4addr | ipv6addr
  [advertised-routes |
```

```
  received prefix-filter |
  received-routes |
  routes]]
```

Parameter	Description
ipv4addr | *ipv6addr*	Network and mask information.
advertised-routes	Displays the routes advertised to a BGP neighbor.
received prefix-filter	Displays all received routes, both accepted and rejected.
received-routes	Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first.
routes	Displays all accepted routes learned from neighbors.

Mode All

show bgp ipv4 prefix-list

Description Display IPv4 routes that match the specified prefix list.

Syntax

```
show bgp ipv4 prefix-list list-name
```

Mode All

show bgp ipv4 quote-regexp

Description Display IPv4 routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).

Syntax

```
show bgp ipv4 quote-regexp string
```

Mode All

show bgp ipv4 summary

Description Display a summary of BGP IPv4 neighbor status.

Syntax

```
show bgp ipv4 summary
```

Mode All

show bgp ipv6

Description Displays BGP information for IPv6.

Syntax

```
show bgp ipv6
[
ipv6addr |
ipv6addr/mask-length |
community [community-number] [options]
  [local-AS] [no-advertise] [no-export] |
community-list list-name [exact-match] |
dampening {dampened-paths | flap-statistics | parameters} |
filter-list list-name |
inconsistent-as |
labeled |
large-community list-name |
large-community-list |
multicast {ipv6addr | ipv6addr/mask-length [longer-prefixes]}
|
neighbors [ipv4addr | ipv6addr
  [advertised-routes | received prefix-filter | received-
routes | routes]] |
paths |
prefix-list list-name |
quote-regexp string |
regexp string [string ...] |
route-map map-name |
summary |
unicast {ipv6addr | ipv6addr/mask-length [longer-prefixes]} |
view view-name
]
```

Parameter	Description
ipv6addr | *ipv6addr/mask-length*	Network and mask information.
community	Displays routes for communities. Enter the

Parameter	Description
[*community-number*] [*options*]	community number in AA:NN format. The following *options* are supported: • **exact-match** – Displays only communities that exactly match. • **local-AS** – Displays only communities that are not sent outside the local AS. • **no-advertise** – Displays only communities that are not sent advertised to neighbors. • **no-export** – Displays only communities that are not exported to the next AS.
community-list list-name [**exact-match**]	Displays routes matching the specified community list. The **exact-match** option displays only the routes that have exactly the same communities.
dampening {options}	displays route-flap dampening information. You must specify one of the following options: • **dampened-paths** – Displays paths suppressed due to dampening. • **flap-statistics** – Displays flap statistics for routes. • **parameters** – Displays details for configured dampening parameters.
filter-list *list-name*	Displays routes that match the specified filter list.
inconsistent-as	Displays routes that have inconsistent AS Paths.
labeled	IPv6 prefix <network>/<length>.
large-community *numXX:YY:ZZ* **exact-match**	Displays routes matching the large communities. Large community number in the format XX:YY:ZZ. The exact-match option displays only the routes that have exactly the same large communities.

Parameter	Description
large-com-munity-list *list-name*	Displays routes matching the large community-list.
neighbors [*ipv4addr* | *ipv6addr* [*options*]]	Displays detailed information about TCP and BGP neighbor connections. The following options are supported: • **advertised-routes** – Displays the routes advertised to a BGP neighbor. • **received prefix-filter** – Displays all received routes, both accepted and rejected. • **received-routes** – Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first. • **routes** – Displays all accepted routes learned from neighbors.
paths	Displays BGP path information.
prefix-list *list-name*	Displays routes that match the specified prefix list.
quote-regexp *string*	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).
regexp *string* [*string ...*]	Displays routes that match the specified AS-path regular expression(s).
route-map *map-name*	Displays routes that match the specified route map.
summary	Displays a summary of BGP neighbor status.
unicast {*ipv6addr* | *ipv6addr*/*mask-*	Displays IPv6 routes for the specified unicast address family. The **longer-prefixes** option includes prefixes that have a longer mask than

Parameter	Description
length [**longer-prefixes**]}	the one specified.
view *view-name*	Displays neighbors within the specified view.

Mode All

show bgp ipv6addr

Description Display BGP network information for IPv6.

Syntax

```
show bgp {ipv6addr | ipv6addr/mask-length [longer-prefixes]}
```

Parameter	Description
ipv6addr | *ipv6addr*/*mask-length*	IPv6 prefix and mask length.
longer-prefixes	Include prefixes that have a longer mask than the one specified.

Mode All

show bgp nexthop-tracking

Description Display the status of nexthop address tracking.

Syntax

```
show bgp nexthop-tracking
```

Mode All

show bgp nexthop-tree-details

Description Use this command to display BGP nexthop-tree details.

Syntax

```
show bgp nexthop-tree-details
```

Mode All

show ip bgp

Description Displays the BGP connections to neighbors.

Syntax

```
show ip bgp
```

Mode All

Example The following example shows output for the `show ip bgp` command when the `asdot` notation is configured:

```
ACOS#show ip bgp
BGP Address Family IPv4 Unicast
BGP table version is 3, local router ID is 10.10.10.198
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal, l - labeled
S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Type Path
*> 197.197.197.197/32
10.10.10.197 0 0 197 1.1 1.0 65535 4 3 2 1 i
*> 198.198.198.198/32
0.0.0.0 100 32768 i

Total number of prefixes 2
```

Example The following example shows output for the `show ip bgp` command when the `asdot-plus` notation is configured:

```
ACOS#show ip bgp
BGP Address Family IPv4 Unicast
BGP table version is 2, local router ID is 10.10.10.198
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal, l - labeled
S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Type Path
```

```
*> 197.197.197.197/32
10.10.10.197 0 0 0.197 1.1 1.0 0.65535 0.4 0.3 0.2 0.1 i
*> 198.198.198.198/32
0.0.0.0 100 32768 i

Total number of prefixes 2
```

show ip bgp attribute-info

Description Display internal attribute hash information.

Syntax

```
show ip bgp attribute-info
```

Mode All

show ip bgp cidr-only

Description Display routes with non-natural network masks.

Syntax

```
show ip bgp cidr-only
```

Mode All

show ip bgp community-info

Description Display all BGP community information.

Syntax

```
show ip bgp community-info
```

Mode All

show ip bgp ipv4addr

Description Display BGP network information for IPv4.

Syntax

```
show ip bgp {ipv4addr | ipv4addr/mask-length [longer-
prefixes]}
```

Parameter	Description
ipv4addr | *ipv4addr*/*mask-length*	IPv4 prefix and mask length.
longer-prefixes	Include prefixes that have a longer mask than the one specified.

Mode All

Example Ths

```
ACOS#show ip bgp 192.10.23.67
BGP table version is 7, local router ID is 80.80.80.80
Status codes: s suppressed, d damped, h history, * valid, >
best,
i internal, S Stale
Origin codes: i - IGP, e - EGP,? - incomplete
Network                 Next Hop         Metric LocPrf Weight Path
S>i10.70.0.0/24         192.10.23.67     0    100      0 ?
S>i30.30.30.30/32       192.10.23.67     0    100      0 ?
S>i63.63.63.1/32        192.10.23.67     0    100      0 ?
S>i67.67.67.67/32       192.10.23.67     0    100      0 ?
S>i172.22.10.0/24       192.10.23.67     0    100      0 ?
S>i192.10.21.0          192.10.23.67     0    100      0 ?
S>i192.10.23.0          192.10.23.67     0    100      0 ?
Total number of prefixes 7
```

show ip bgp scan

Description Display BGP scan status.

Syntax

```
show ip bgp scan
```

Mode All

Example Below is an example output for this command.

```
ACOS#show ip bgp scan
BGP scan is running
BGP scan interval is 60
```

```
BGP instance: AS is 11,DEFAULT
Current BGP nexthop cache:
BGP connected route:
10.10.10.0/24
10.10.11.0/24
```

show ip bgp view

Description Display neighbors of a specific view.

Syntax

```
show ip bgp view view-name
[
ipv4addr |
ipv4addr/mask-length |
ipv4 {multicast | unicast} summary |
neighbors [ipv4addr | ipv6addr] |
summary
]
```

Parameter	Description
view-name	Name of the view.
ipv4addr | *ipv4addr*/*mask-length*	Prefix and mask.
ipv4 {**multicast** | **unicast**} **summary**	Displays information for the specified IPv4 address family.
neighbors [*ipv4addr* | *ipv6addr*]	Displays information for the specified neighbor.
summary	Displays summary neighbor information.

Mode All

show ip isis [tag] route

Description Display the IPv4 IS-IS route table.

Syntax

```
show ip isis [tag] route
```

Parameter	Description
System wide total number of IS-IS IPv4 routes	
Code	C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, D - discard, e - external metric
Destination	
Metric	
Next-Hop	
Interface	
Tag	

Replace *tag* with the IS-IS tag (area). If you do not specify a tag value, IPv4 routes for all areas are displayed.

Mode All

Example The following command shows the IPv4 IS-IS route table:

```
ACOS(config)#show ip isis route
System wide total number of IS-IS IPv4 routes is 1 (Limit
8192)
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 -
IS-IS level-2 ia - IS-IS inter area, D - discard, e - external
metric
Area (null):
Destination     Metric  Next-Hop   Interface      Tag
C 1.0.3.0/24     10          --    ethernet 5      --
L11.0.4.0/24     20     12.0.0.2   ethernet 2      0
C12.0.0.0/24     10          --    ethernet 2      --
```

show ip ospf border-routers

Description Display route information for OSPFv2 ABRs and ASBRs.

Syntax `show ip ospf border-routers`

Mode Privileged EXEC and all configuration levels

Example The following command shows route information for ABRs and ASBRs:

```
ACOS#show ip ospf border-routers

OSPF process 0 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 9.1.1.1 [10] via 10.1.1.2, ethernet 1, ASBR, Area 0.0.0.0

OSPF process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route
```

show ip ospf database

Description Displays information about the OSPFv2 databases on the device.

NOTE: The options are different for OSPFv3.

Syntax

```
show ip ospf database
[
adv-router ipaddr |
{asbr-summary | external | network | nssa-external |
  opaque-area | opaque-as | opaque-link | router | summary}
    [[ipaddr [adv-router ipaddr] [self-originate]] |
    [adv-router ipaddr] | [self-originate]] |
       max-age |
       self-originate
]
```

Parameter	Description
adv-router *ipaddr*	Displays LSA information for the specified advertising router.
asbr-summary	Displays information about ASBR summary LSAs.

Parameter	Description
max-age	Displays information for the LSAs that have reached the maximum age allowed, which is 3600 seconds.
self-originate	Displays information for LSAs originated by this OSPF router.
external	Displays information about external LSAs.
network	Displays information about network LSAs.
nssa-external	Displays information about NSSA external LSAs.
opaque-area	Displays information about Type-10 Opaque LSAs. Type-10 Opaque LSAs are LSAs with local-area scope (link state type 10), and are not flooded outside the local area.
opaque-as	Displays information about Type-11 LSAs, which are flooded throughout the Autonomous System (AS).
opaque-link	Displays information about Type-9 LSAs. Type-9 LSAs have link-local scope, and are not flooded beyond the local network.
router	Displays information about router LSAs.
summary	Displays information about summary LSAs.

The following suboptions are available for the **external**, **network**, **nssa-external**, **opaque-area**, **opaque-as**, **opaque-link**, **router**, and **summary** options:

Parameter	Description
ipaddr	Displays LSA information for a specific link-state ID (expressed as an IP address).
adv-router *ipaddr*	Displays LSA information for the specified advertising router.
self-originate	Displays information for LSAs originated by this OSPF router.

Mode Privileged EXEC and all configuration levels

Example The following command shows the OSPFv2 database:

```
ACOS#show ip ospf database

                Router Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Link
count
1.1.1.1         1.1.1.1         1105 0x800000c9 0xcb72 2
2.2.2.2         2.2.2.2          638 0x80000008 0xdb92 2
3.3.3.3         3.3.3.3         1998 0x800000cb 0x47c1 2
4.4.4.4         4.4.4.4         1717 0x800000f6 0xe1d2 3

                Net Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum
10.0.0.1        3.3.3.3         1998 0x80000006 0xec1b
11.0.0.1        3.3.3.3          203 0x80000005 0x14ef
13.0.0.2        4.4.4.4         1717 0x80000006 0xbf3c
14.0.0.1        4.4.4.4         1962 0x80000004 0xf207

                Summary Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         3.3.3.3         1998 0x800000a3 0x99ed
0.0.0.0/0

                NSSA-external Link States (Area 0.0.0.1
[NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
           Tag
1.0.100.1       1.1.1.1         1105 0x8000008e 0x942a E2
1.0.100.1/32    0
```

show ip ospf redistributed

Description Display the routes that are being redistributed into OSPFv2.

Syntax

```
show ip ospf [process-id] redistributed
[
bgp |
connected |
floating-ip |
ip-nat |
ip-nat-list |
isis |
kernel |
lw4o6 |
ospf [|process-id] |
rip
selected-vip
static |
vip
]
```

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPF processes is displayed.
bgp	Displays redistributed routes from BGP.
connected	Displays redistributed routes to directly-connected networks.
floating-ip	Displays redistributed routes to floating IP addresses.
ip-nat	Displays redistributed routes to IP addresses assigned from an IP NAT pool.
ip-nat-list	Displays redistributed routes to IP addresses assigned from an IP NAT range list.
isis	Displays redistributed routes from IS-IS.
kernel	Displays redistributed kernel routes.
lw4o6	Displays redistributed Lightweight 4over6 routes.
ospf [*process-id*]	Displays redistributed routes from other OSPFv2 processes.
rip	Displays redistributed routes from RIP.
selected-vip	Displays redistributed routes to SLB VIPs that are explicitly flagged for redistribution. This option is

Parameter	Description
	applicable if the only-flagged option was used with the redistribute vip command.
static	Displays redistributed static routes.
vip	Displays redistributed routes to SLB VIPs that are implicitly flagged for redistribution. This option is applicable if the only-not-flagged option was used with the redistribute vip command.

Mode Privileged EXEC and all configuration levels

show ip rip database

Description Display the RIP IPv4 route database.

Syntax

```
show ip rip database
```

Mode All

Example The following command displays the IPv4 RIP database:

```
ACOS(config)# show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K -
Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B -
BGP,
       v - VIP, V - VIP selected, N - IP NAT group,
       n - IP NAT, f - Floating IP

   Network            Next Hop         Metric From
If     Time
Rc 1.0.3.0/24                              1
ethernet 5
R  1.0.4.0/24         12.0.0.2             2 12.0.0.2
ethernet 2 02:59
Rc 12.0.0.0/24                             1
ethernet 2
```

Parameter	Description
Codes	• R - RIP • Rc - RIP connected • Rs - RIP static • K - Kernel • C - Connected • S - Static • O - OSPF • I - IS-IS • B - BGP, • v - VIP • V - VIP selected • N - IP NAT group, • n - IP NAT • f - Floating IP
Network	Destination network and subnet mask.
Next Hop	Next hop IP address.
Metric	Cost of the route.
From	IP address of the originating router.
If	Outgoing interface.
Time	Remaining lifetime of the route.

show ip route acos

Description Display ACOS information in the routing table.

Syntax

```
show ip route acos
```

Mode EXEC

Example The following command shows the sample output:

```
ACOS#show ip route acos

Codes: V - VIP, VF - VIP Flagged, N - IP NAT
       NR - IP NAT Range List, F - Floating IP
       N64 - NAT64, LW - LW4o6
VF     5.5.5.5/32 (appl-redist-rmap RMAP)
VF     6.6.6.6/32
```

show ipv6 isis [tag] route

Description Display the IPv6 IS-IS route table.

Syntax

```
show ipv6 isis [tag] route
```

Parameter	Description
System wide total number of IS-IS IPv6 routes	
Code	C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, D - discard, e - external metric
Destination	
Metric	
Next-Hop	
Interface	
Tag	

Replace *tag* with the IS-IS tag (area). If you do not specify a tag value, IPv6 routes for all areas are displayed.

Mode All

Example The following command shows the IPv6 IS-IS route table:

```
ACOS(config)#show ipv6 isis route
System wide total number of IS-IS IPv6 routes is 1 (Limit
8192)
```

```
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Area (null):
C     3000::/64 [10]
       via ::, ethernet 2
C     3ff3::/64 [10]
       via ::, ethernet 5
L1    3ff4::/64 [20]
       via fe80::21f:a0ff:fe10:a4a6, ethernet 2
```

show ipv6 isis [tag] topology

Description Display IPv6 IS-IS topology information.

Syntax

```
show ipv6 isis [tag] topology [l1 | l2 | level-1 | level-2]
```

Parameter	Description
tag	Specifies the IS-IS tag (area). If you do not specify a tag value, topology information for all areas is displayed.
l1 | **l2** | **level-1** | **level-2**	Specifies the IS-IS routing level for which to display topology information. The default is **level-1**.
System Id	
Metric	
Next-Hop	
Interface	
SNPA	

Mode All

Example The following command shows IPv6 IS-IS topology information:

```
ACOS(config)#show ipv6 isis topology
Area (null):
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface
  SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       ethernet
2  001f.a010.a4a6

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface
  SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       ethernet
2  001f.a010.a4a6
```

show ipv6 ospf database

Description Displays information about the OSPFv3 databases on the device.

Syntax

```
show ipv6 ospf [tag] database
[
external [adv-router ipaddr] |
grace [adv-router ipaddr] |
inter-prefix [adv-router ipaddr] |
inter-router [adv-router ipaddr] |
intra-prefix [adv-router ipaddr] |
link [adv-router ipaddr] |
network [adv-router ipaddr] |
router [adv-router ipaddr]
]
```

Parameter	Description
external	Displays information about external LSAs.
inter-prefix	Displays information about Inter-Area-Prefix LSAs.
inter-router	Displays information about Inter-Area-Router LSAs.
intra-prefix	Displays information about Intra-Area-Prefix LSAs.

Parameter	Description
links	Displays information about link LSAs.
network	Displays information about network LSAs.
router	Displays information about router LSAs.
[adv-router] *ipaddr*	Displays LSA information for the specified advertising router.

Mode Privileged EXEC and all configuration levels

Example The following command shows the OSPFv3 database:

```
ACOS#show ipv6 ospf database

            OSPFv3 Router with ID (100.1.1.1) (Process *null*)
                Link-LSA (Interface ethernet 1)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.3         9.1.1.1          498 0x8000000c 0xfa01      1
0.0.0.3         100.1.1.1         31 0x80000001 0xf29e      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum    Link
0.0.0.0         9.1.1.1           19 0x8000000d 0x9356      1
0.0.0.0         100.1.1.1         18 0x80000003 0x7127      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.3         9.1.1.1           19 0x80000001 0x7d29

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
Reference
0.0.0.2         9.1.1.1           18 0x80000001 0x5d5f      1
Network-LSA

                AS-external-LSA
```

```
Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.4         9.1.1.1         1508 0x80000017 0x6aad E2
0.0.0.1         100.1.1.1         29 0x80000001 0xcd18 E2
```

show ipv6 ospf topology

Description Display OSPFv3 topology information.

Syntax

```
show ipv6 ospf [tag] topology [area area-id]
```

Parameter	Description
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes is displayed.
area *area-id*	Displays OSPFv3 topology information for the specified area.

Mode Privileged EXEC and all configuration levels

Example The following command shows the OSPFv3 topology:

```
ACOS#show ipv6 ospf topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop
Interface
9.1.1.1            E   10         9.1.1.1
ethernet 1
100.1.1.1          E   --
```

show ipv6 rip database

Description Display the RIP IPv4 route database.

Syntax

```
show ipv6 rip database
```

Mode All

Example The following command displays the IPv6 RIP database:

```
ACOS(config)# show ipv6 rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP
aggregated,
       Rcx - RIP connect suppressed, Rsx - RIP static
suppressed,
       K - Kernel, C - Connected, S - Static, O - OSPF, I -
IS-IS, B - BGP,
       v - VIP, V - VIP selected, N - IP NAT group,
       n - IP NAT, f - Floating IP

     Network                    Next Hop                   If
    Met Tag  Time
Rc   3000::/64                  ::
ethernet 2  1   0
Rc   3ff3::/64                  ::
ethernet 5  1   0
R    3ff4::/64                  fe80::21f:a0ff:fe10:a4a6
ethernet 2  2   0 02:59
```

Parameter	Description
Codes	• R - RIP • Rc - RIP connected • Rs - RIP static • Ra - RIP aggregated • Rcx - RIP connect suppressed • Rsx - RIP static suppressed • K - Kernel • C - Connected • S - Static • O - OSPF • I - IS-IS • B - BGP,

Parameter	Description
	• v - VIP • V - VIP selected • N - IP NAT group, • n - IP NAT • f - Floating IP
Network	Destination network and subnet mask.
Next Hop	Next hop IP address.
If	Outgoing interface.
Metric	Cost of the route.
Tag	Tag information of the route.
Time	Remaining lifetime of the route.

show isis [tag] database

Description Display the IS-IS database entries.

Syntax

```
show isis [tag] database
[lspid]
[detail | verbose]
[l1 | l2 | level-1 | level-2]
```

Parameter	Description
tag	Specifies the IS-IS tag (area). If you do not specify a tag value, database entries for all areas is displayed.
lspid	Specifies the ID of a specific LSP to display.
detail	Displays detailed contents of the LSPs. Without this option, summary information is displayed.
verbose	Displays verbose database information.
l1 | **l2** | **level-1** | **level-2**	Specifies the IS-IS routing level for which to display database entries. The default is **level-1**.

Mode All

Example The following command shows the IS-IS database:

```
ACOS(config)#show isis database
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime
    ATT/P/OL
0000.0000.0001.00-00* 0x00000007   0x8223        857
    0/0/0
0000.0000.0002.00-00  0x00000007   0x0F96        865
    0/0/0
0000.0000.0002.02-00  0x00000004   0x01D4        865
    0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime
    ATT/P/OL
0000.0000.0001.00-00* 0x00000003   0x77F4        884
    0/0/0
0000.0000.0002.00-00  0x00000003   0x640A        879
    0/0/0
0000.0000.0002.02-00  0x00000001   0x07D1        853
    0/0/0
```

show isis [tag] topology

Description Display IPv4 IS-IS topology information.

Syntax

```
show isis topology [l1 | l2 | level-1 | level-2]
```

You can specify one of **l1**, **l2**, **level-1**, or **level-2** as the IS-IS routing level for which to display topology information.

Parameter	Description
Area	
System Id	
Metric	

Parameter	Description
Next-Hop	
Interface	
SNPA	

Default `level-1`

Usage All

Example The following command shows IPv4 IS-IS topology information:

```
ACOS(config)#show isis topology

Area (null):
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface
  SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       ethernet
2  001f.a010.a4a6

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface
  SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       ethernet
2  001f.a010.a4a6
ACOS(config)#
```

show isis counter

Description Display IS-IS statistics.

Syntax

```
show isis counter
```

Parameter	Description
IS-IS Level-1	
IS-IS Level-2	

Mode All

Example The following command shows IS-IS counters:

```
ACOS(config)#show isis counter
Area (null):
IS-IS Level-1 isisSystemCounterEntry:
  isisSysStatCorrLSPs: 0
  isisSysStatAuthTypeFails: 0
  isisSysStatAuthFails: 0
  isisSysStatLSPDbaseOloads: 0
  isisSysStatManAddrDropFromAreas: 0
  isisSysStatAttmptToExMaxSeqNums: 0
  isisSysStatSeqNumSkips: 0
  isisSysStatOwnLSPPurges: 0
  isisSysStatIDFieldLenMismatches: 0
  isisSysStatMaxAreaAddrMismatches: 0
  isisSysStatPartChanges: 0
  isisSysStatSPFRuns: 4

IS-IS Level-2 isisSystemCounterEntry:
  isisSysStatCorrLSPs: 0
  isisSysStatAuthTypeFails: 0
  isisSysStatAuthFails: 0
  isisSysStatLSPDbaseOloads: 0
  isisSysStatManAddrDropFromAreas: 0
  isisSysStatAttmptToExMaxSeqNums: 0
  isisSysStatSeqNumSkips: 0
  isisSysStatOwnLSPPurges: 0
  isisSysStatIDFieldLenMismatches: 0
  isisSysStatMaxAreaAddrMismatches: 0
  isisSysStatPartChanges: 0
  isisSysStatSPFRuns: 3
```

show isis interface

Description Display IS-IS information for interfaces.

Syntax

```
show isis interface
[
counter |
ethernet port-num |
lif num |
loopback num |
trunk num |
ve ve-num
}
```

Parameter	Description
counter	Displays IS-IS interface status information and statistics.
ethernet *port-num*	Displays IS-IS information for the specified Ethernet data port.
lif *num*	Displays IS-IS information for the specified logical interface.
loopback *num*	Displays IS-IS information for the specified loopback interface.
trunk *num*	Displays IS-IS information for the specified trunk interface.
ve *ve-num*	Displays IS-IS information for the specified VE interface.

Mode All

Example The following command shows IS-IS interface information:

```
ACOS(config)#show isis interface
ethernet 2 is up, line protocol is up
  Routing Protocol: IS-IS ((null))
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000005
    Local SNPA: 001f.a002.5bc9
```

```
    MTU: 1500 (Jumbo enabled)
    IP interface address:
      12.0.0.1/24
    IPv6 interface address:
      3000::1/64
      fe80::21f:a0ff:fe02:5bc9/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID:
0000.0000.0002.02
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10/10, Priority: 64, Circuit ID:
0000.0000.0002.02
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 4 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
ethernet 5 is up, line protocol is up
  Routing Protocol: IS-IS ((null))
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x0000000B
    Local SNPA: 001f.a002.5bcc
    MTU: 1500 (Jumbo enabled)
    IP interface address:
      1.0.3.1/24
    IPv6 interface address:
      3ff3::1/64
      fe80::21f:a0ff:fe02:5bcc/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID:
0000.0000.0001.02
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10/10, Priority: 64, Circuit ID:
0000.0000.0001.02
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 3 seconds
    Next IS-IS LAN Level-2 Hello in 3 seconds
```

show virtual-wire-global

Description Display the current active VLAN members in a bridge-vlan-group and the global counters.

Syntax

```
show virtual-wire-global { counters | vlan-group-active-member
| vlan-set-active-member}
```

Parameter	Description
counters	Displays the global counters. These counters indicate the number of times the VLAN and MAC information has been updated. When the MAC address changes within the same session, the MAC counter increments.
vlan-group-active-member	Displays the current active VLAN members in a bridge-vlan-group.
vlan-set-active-member	Displays the active VLAN pairs in virtual-wire-vlan-pair-set.

Mode Configuration Mode

Example The following command displays the current active VLAN members in a bridge-vlan-group:

```
ACOS(config)# show virtual-wire-global vlan-group-active-
member
bridge-vlan-group:    1
active vlan      :   20
```

Example The following command displays the global counters:

```
ACOS(config)# show virtual-wire-global counters
VLAN update     : 0
MAC update      : 0
VLAN pair update: 0
standby drop    : 2
```

Parameter	Description
VLAN update	Displays the counters of the global VLAN update.
MAC update	Displays the counters of the global MAC address update.
vlan pair update	Displays the counters of the VLAN pairs in virtual-wire-vlan-pair-set.
standby drop	Displays the counter of the packet dropped due to VLAN in the standby mode.

show virtual-wire-health-check

Description Display the health check statistics and active VLAN members in a virtual-wire.

Syntax

```
show virtual-wire-health-check { statistics | vlan id [statistics]}
```

Parameter	Description
statistics	Displays the health check entry status for all VLANs.
vlan *id*	Displays the heath check entry status for the specified VLAN ID.
vlan *id* **statistics**	Displays the statistics for the specified VLAN ID to track active and standby events.

Mode Configuration Mode

Example The following command displays the health check entry status all the VLAN:

```
ACOS(config)#show virtual-wire-health-check statistics
Entry VLAN: 20
Entry state: Enabled
VLAN state: Active

Entry VLAN: 30
Entry state: Disabled
VLAN state: Active

Entry VLAN: 40
Entry state: Enabled
VLAN state: Standby
```

Example The following command displays the statistics for specific VLAN ID to track active and standby events:

```
ACOS(config)#show virtual-wire-health-check vlan 40 statistics
Entry VLAN: 40
Active event: 0
Standby event: 1
```

Overlay Networks

An overlay network is a virtual network built on top of an existing physical network in order to introduce a service that is not available in that existing network. The overlay network uses virtual links to connect various nodes of the existing physical network. Virtual network traffic is then tunneled across the network using technologies like VXLAN (Virtual Extensible LAN) and NVGRE (Network Virtualization using Generic Routing Encapsulation).

This reference lists the CLI configuration and show commands that apply specifically to overlay network.

Configuration Commands

debug packet

Description Shows the extended details of the encapsulated tunnel payload.

Syntax

```
debug packet {count | detail | interface | l3-protocol | l4-protocol}
```

Parameter	Description
`count`	The count of the maximum packets to capture. Default is 3000.
`detail`	Print packet content.
`interface`	Specify the ethernet interface number to debug.
`l3-protocol`	Layer 3 protocol (ARP, IP, IPv6, IPv6 neighbor/Router).
`l4-protocol`	Layer 4 protocol (ICMP, ICMPv6, TCP, UDP).

Default N/A

Mode Enable mode.

Usage

To see encapsulated packets with the appropriate headers, use **debug packet** in the underlay/provider partition.

To see de-encapsulated packets, use **debug packet** in the overlay/tenant partition.

If both underlay and overlay are mapped to the same partition, this command will show both encapsulated and decapsulated packets.

Example

The following output is an example of the **debug packet** command in the underlay/provider partition.

```
ACOS# debug packet l3-protocol ip all
Wait for debug output, enter <ctrl c> to exit
@312173 i( 1, 100, 222c8)> ip 90.1.1.1 > 100.1.1.2 udp 44221 >
4789 len 76 vxlan/vni 100 arp who-has 80.1.1.10 tell
80.1.1.100
@312173 o( 1, 100, 222c8)> ip 100.1.1.2 > 90.1.1.1 udp 44221 >
4789 len 58 vxlan/vni 100 arp reply 80.1.1.10 is-at
00:0d:48:0a:66:5e tell 80.1.1.100
@312173 i( 1, 100, 222c9)> ip 90.1.1.1 > 100.1.1.2 udp 4015 >
4789 len 114 vxlan/vni 100 ip 80.1.1.100 > 80.1.1.10 icmp echo
req seq=1
@312173 i(32, 1, 222c9)> ip 80.1.1.100 > 80.1.1.10 icmp echo
req seq=1
@312173 o(32, 1, 222c9)> ip 80.1.1.10 > 80.1.1.100 icmp echo
rsp seq=1
@312173 o( 1, 100, 222c9)> ip 100.1.1.2 > 90.1.1.1 udp 62284 >
4789 len 114 vxlan/vni 100 ip 80.1.1.10 > 80.1.1.100 icmp echo
rsp seq=1
```

The **bold** portions of the output show details about the encapsulated overlay tunnel packets.

The following show details about the decapsulated packets:

```
@312173 i(32, 1, 222c9)> ip 80.1.1.100 > 80.1.1.10 icmp echo
req seq=1
@312173 o(32, 1, 222c9)> ip 80.1.1.10 > 80.1.1.100 icmp echo
rsp seq=1
```

interface lif

Description Configures a Layer 2 logical tunnel interface (LIF); this is an extension of the existing interface command. As a Layer 2 interface, the LIF will forward all unknown unicast, multicast, and broadcast packets to all destination VTEPs on the same VNI.

The LIF can additionally have an IP address configured on it, thus making it a Layer 3 interface. As a Layer 3 interface:

- Unicast traffic causes an ARP request to be generated and flooded to all remote VTEPs on the same VNI.
- Multicast and broadcast traffic are dropped.

Syntax

```
[no] interface lif lif-num
```

Replace *lif-num* with the number of the logical interface.

Default N/A

Mode Configuration mode.

Example Configure a logical interface number 1:

```
ACOS(config)# interface lif 1
ACOS(config-if:lif:1)#
```

Related Commands:

- untagged lif

overlay-mgmt-info

Description Configure the connection string used by the SCVMM plugin or other machine manager plugins on the ACOS device.

Syntax

```
[no] overlay-mgmt-info plugin-string application-string
```

Parameter	Description
plugin-string	Configure the plugin string (1-128 characters).

Parameter	Description
application-string	Configure the application string (1-128 characters).

Mode Configuration mode.

Usage This command can only be used in the shared partition; it is not supported in L3V partitions.

Example The following example configures “nvgre” as the plugin string and “a10networks” as the application string:

```
ACOS(config)# overlay-mgmt-info nvgre a10networks
```

Related Commands:

- show running-config overlay-mgmt-info

overlay-tunnel vtep

Description Top-level command to begin the configuration of the overlay tunnel. This command enables you to create a virtual tunnel endpoint (VTEP). Multiple VTEPs can be configured in the same partition or across different partitions.

Syntax

```
[no] overlay-tunnel vtep vtep-id
{
   dest-port mac-address |
   encap port |
   host |
   local-ip-address |
   local-ipv6-address |
   remote-ip-address |
   remote-ipv6-address |
   sampling-enable |
   src-port-range
}
```

Default N/A

Mode Configuration mode.

Usage If the ACOS device is a member of an aVCS, use the **device-context** command to specify the device in the Multi-PU platform to which this command must apply.

Example The following example configures a VTEP with the ID of 1.

```
ACOS(config)# overlay-tunnel vtep 1
```

Example The following example removes a tunnel configuration (you are prompted to confirm the command).

```
ACOS(config)# no overlay-tunnel vtep 1
This command will delete the entire overlay-tunnel and related
sub-configuration. Proceed with deleting it? [yes/no] yes
ACOS(config)#
```

Related Commands:

- encap
- host
- local-ip-address
- remote-ip-address
- src-port-range

encap

Description When used in Overlay Tunnel VTEP mode, this command sets the type of encapsulation you want to use for tunnelling packets.

When used in the Destination VTEP mode, it specifies the encapsulation type for that specific destination VTEP and overrides any prior encapsulation specification.

In either case, this command is optional and is not required for configuring an overlay tunnel.

Syntax `encap {ip-encap | gre | nvgre | vxlan}`

Default vxlan

Mode Overlay Tunnel VTEP mode or Destination VTEP mode.

Example Specify `nvgre` as the encapsulation type for the tunnel.

```
ACOS(config-overlay-tunnel:1)# encap nvgre
```

Specify `vxlan` as the encapsulation type for the destination VTEP and override any prior encapsulation specification.

```
ACOS(config-overlay-tunnel:1-dst-vtep)# encap vxlan
```

Specify `ip-encap` as encapsulation type for the destination VTEP for both IPv4 and IPv6 encapsulation.

```
ACOS(config-overlay-tunnel:1-dst-vtep)# encap ip-encap
```

Specify `gre` as the encapsulation type for the destination VTEP IPv4 GRE tunnelling encapsulation.

```
ACOS(config-overlay-tunnel:1-dst-vtep)# encap gre
```

host

Description Maps the host to a specific VTEP and VNI/VSID. This is an optional command to configure host mapping if dynamic learning is not desired.

NOTE: For NVGRE, static mapping with the **host** command is mandatory; dynamic learning is not supported.

With dynamic learning, ARP packets are flooded to all configured destination VTEPs that are configured for the same VNI for this source VTEP until an ARP response or another packet comes from that host via one of the destination VTEP tunnels. The source VTEP then learns the host-to-destination VTEP mapping and uses it for subsequent packet forwarding.

Static mapping with the **host** command is recommended if you want to avoid the overhead associated with dynamic learning.

Syntax

```
host [host-ip] host-mac vni overlay-segment-id {remote-vtep
ip-address | remote-ipv6-vtep ip-address}
```

Parameter	Description
host *[host-ip]*	Optional parameter specifying the IP address of the host across the tunnel. This is used when the logical interface is configured as a Layer 3 interface and

Parameter	Description
	causes a static ARP entry to be added to the LIF partition corresponding to the host IP address.
host-mac	The MAC address of the overlay host.
vni *overlay-segment-id*	The segment being extended (1-16777215).
remote-vtep *ip-address* | **remote-ipv6-vtep** *ip-address*	The IPv4 or IPv6 address of the remote VTEP.

Default N/A

Mode Overlay Tunnel VTEP mode.

Example The following command maps the host with the MAC address of 001a.112b.223c to VNI 100, located behind the destination VTEP with the IP address 100.1.1.10.

```
ACOS(config-overlay-tunnel:1)# host 001a.112b.223c vni 100
destination-vtep 100.1.1.10
```

The following example maps the host with the MAC address of 001a.002a.003a to the destination host with the IP address 30.1.1.20. The destination host is on VNI 200 and is located behind the destination VTEP with the IP address 110.1.1.10.

```
ACOS(config-overlay-tunnel:1)# host 30.1.1.20 001a.002a.003a
vni 200 destination-vtep 110.1.1.10
```

local-ip-address

Description Specify the source or local IP address of the VTEP on the underlay network.

NOTE: The IP address used in the configuration must be present in the underlay partition as an interface IP or a floating IP before traffic flow is functional.

Syntax

```
local-ip-address ipv4-address
local-ipv6-address ipv6-address
```

Parameter	Description
local-ip-address *ipv4-address*	Specify the source IPv4 address of the VTEP.
local-ipv6-address *ipv6-address*	Specify the source IPv6 address of the VTEP.

Mode Overlay Tunnel VTEP mode.

Example The following example shows a VTEP with 90.1.1.1 as the local IP address:

```
ACOS(config)# overlay-tunnel vtep 1
ACOS(config-overlay-tunnel:1)# local-ip-address 90.1.1.1
```

Related Commands:

- remote-ip-address

remote-ip-address

Description Specify the remote VTEP IP address of the destination tunnel endpoint.

Syntax

```
remote-ip-address ipv4-address [class-list name]
remote-ipv6-address ipv6-address [class-list name]
```

Parameter	Description
remote-ip-address *ipv4-address*	Specify the IPv4 address of the destination tunnel endpoint. If you want to allow any IP address from the

Parameter	Description
	network, provide the default IP address (0.0.0.0) as a remote VTEP IPv4 address.
remote-ipv6-address *ipv6-address*	Specify the IPv6 address of the destination tunnel endpoint. If you want to allow any address from the network, provide the default IP address (0:0:0:0:0:0 or 0::0) as a remote VTEP IPv6 address.
class-list *name*	Specify the name of the pre-configured class-list (for IP limiting). The class-list is used to filter the IPv4 or IPv6 addresses that are allowed in the adhoc tunnel. For more information, see the **Usage** section and *Configuring Overlay Networks* guide. **NOTE:** The class-list filter is allowed only with the default IP address and not with any non-zero IPv4 or IPv6 addresses.

Mode Overlay Tunnel VTEP mode.

Usage In the point-to-point tunnel configuration, a remote IP address can be any non-zero IP address defined as a VTEP.

In the point-to-multipoint tunnel configuration, a remote IP address has a default IP address (0.0.0.0 or 0::0) with or without the class-list filter. An adhoc tunnel is created in an overlay network using such a remote IP address with GRE and IPinIP encapsulation. In the adhoc tunnel configuration, a dedicated unique Logical Interface (LIF) is configured to hold multiple remote tunnel endpoints. A local IP address is configured for every remote tunnel endpoint and every overlay tunnel in the partition.

The adhoc tunnel always originates from the remote tunnel endpoint and ends at the local IP address. Each remote endpoint connected to

the Thunder device through an adhoc tunnel must have a unique IP address.

NOTE: GRE keepalive is not supported on adhoc tunnels.

Example The following example shows the destination VTEP with a non-zero IP address in a point-to-point tunnel configuration.

```
ACOS(config)# overlay-tunnel vtep 1
ACOS(config-overlay-tunnel:1)# remote-ip-address 90.1.1.2
```

The following example shows the adhoc tunnel configuration that allows any IP address in the overlay network using IPinIP encapsulation.

```
ACOS(config)# overlay-tunnel vtep 1
ACOS(config-overlay-tunnel:1)# encap ip-encap
ACOS(config-overlay-tunnel:1)# local-ip-address 165.165.165.1
ACOS(config-overlay-tunnel:1)# remote-ip-address 0.0.0.0
ACOS(config-overlay-tunnel:1-dst-vtep:0.0.0.0)# lif 100
ACOS(config-overlay-tunnel:1-dst-vtep:0.0.0.0)# exit
ACOS(config-overlay-tunnel:1)# exit
ACOS(config)#
```

The following example shows the adhoc tunnel with class-list configuration using GRE encapsulation.

```
ACOS(config)# class-list INTERNAL
ACOS(config-class list)# 99.0.1.0/24 lsn-lid 1
ACOS(config-class list)# 172.16.231.0/24 lsn-lid 1
ACOS(config-class list)# exit
ACOS(config)# overlay-tunnel vtep 3
ACOS(config-overlay-tunnel:3)# encap gre
ACOS(config-overlay-tunnel:3)# local-ip-address 165.165.165.1
ACOS(config-overlay-tunnel:3)# remote-ip-address 0.0.0.0
class-list INTERNAL
ACOS(config-overlay-tunnel:3-dst-vtep:0.0.0.0)# lif 100
ACOS(config-overlay-tunnel:3-dst-vtep:0.0.0.0)# exit
ACOS(config-overlay-tunnel:3)# exit
ACOS(config)#
```

Related Commands:

- local-ip-address

src-port-range

Description Configures the layer 4 (UDP) source port range per VTEP for VXLAN overlay tunnels.

Syntax

```
[no] src-port-range min-port num max-port num
```

Parameter	Description
min-port *num*	Specify the minimum port number. The range can be from 1-65535.
max-port *num*	Specify the maximum port number. The range can be from 1-65535.

Default N/A

Mode Overlay Tunnel VTEP mode.

Usage ACOS selects the VXLAN UDP source (SRC) ports based on the following conditions:

- If you do not configure a VTEP with a SRC port range, the VTEP uses the global SRC port range configured.
- Changing a VTEP SRC port range takes effect immediately, removing existing sessions in the VTEP and changes the VTEP to use the new SRC port range.
- If you change the global VXLAN UDP SRC port range, then existing VTEPs do not inherit the new SRC port range; only new VTEPs configured after the change will inherit the new SRC port range to prevent disruptions to existing VTEP sessions.

NOTE: For all existing VTEPs to use a configured global UDP SRC port range, save the configuration using the **write memory** command and reboot the device using the **reload** or **reboot** commands.

Example The following example configures the source port range on a VTEP.

```
ACOS(config)# overlay-tunnel vtep 1
```

```
ACOS(config-overlay-tunnel:1)# src-port-range min-port 1000
max-port 2000
```

Example The following example configures VTEP 20, UDP SRC-port range 2000 to 3000, virtual network ID, VNI 10, and the remote endpoint IP address. Configure the LIF interface before configuring the VNI.

```
ACOS(config)# overlay-tunnel vtep 20
ACOS(config-overlay-tunnel:20)# encap nvgre
ACOS(config-overlay-tunnel:20)# src-port-range min-port 2000
max-port 3000
ACOS(config-overlay-tunnel:20)# local-ip-address 10.1.1.1
ACOS(config-overlay-tunnel:20-src-vtep:10....)# vni 10 lif 1
ACOS(config-overlay-tunnel:20-src-vtep:10....)# exit
ACOS(config-overlay-tunnel:20)# remote-ip-address 203.0.113.10
```

Related Commands:

- src-port-range

vni

Description Configures the VXLAN Network Identifier (VNI) or NVGRE Virtual Subnet Identifier (VSID) of the segment that is being extended across the network when used at the Main Tunnel VTEP submode.

Specifies the VNI or VSID of the remote VTEP when used at the Remote VTEP submode.

Syntax

```
Overlay Tunnel VTEP mode:
vni overlay-segment-id [partition overlay-partition-name] lif
logical-interface-id [gateway]

Destination VTEP mode:
vni overlay-segment-id
```

Parameter	Description
vni *overlay-segment-id*	When used following local-ip-address, this command configures the VNI/VSID (1-16777215) of the segment that is being extended across the network. When used following remote-ip-address, this

Parameter	Description
	command specifies the VNI/VSID of the destination VTEP.
partition *overlay-partition*	The partition containing the hosts/configuration for the overlay network. This is an optional parameter; if not specified, it defaults to the partition where this configuration is being done.
lif *logical-interface-id*	The logical interface (LIF) number which acts as a conduit interface to/from the tunnel network. A given LIF in a partition can map to only a single VNI in the system. The only exception is when a gateway VSID has been configured for that LIF.
gateway	Optional parameter to make the configured VNI a gateway. This is typically used in NVGRE deployments, where a Hyper-V host is configured to use a specific VNI that corresponds to a default gateway. In terms of packet handling, an ACOS device can receive packets on a gateway VNI but will always transmit packets on the regular VSID. In some implementations, traffic from a host can be received on a different VNI than the one on which it was sent. The gateway VNI serves to support this communication. Once a gateway VNI is configured for a LIF, multiple VNIs (called regular VNIs) can be configured under same LIF. In this case, packets are sent out over the tunnel using regular VNIs and are expected to be received on gateway VNI. The host command is needed to resolve the ambiguity of which VNI to use while sending packets over the tunnel.

Parameter	Description
	Multiple VNIs under same LIF cannot be configured unless the LIF is carrying a gateway VNI. There can be multiple gateway VNIs under a given VTEP (each with a different LIF).

Default N/A

Mode Overlay Tunnel VTEP mode or Destination VTEP mode.

Example Configure a VNI with an ID of 100, specify p1 as the partition, and 10 as the logical interface ID:

```
ACOS(config-overlay-tunnel:1-src-vtep)# vni 100 partition p1
lif 10
```

Configure the destination VTEP VNI of 200:

```
ACOS(config-overlay-tunnel:1-dst-vtep)# vni 200
```

The example below shows how to configure multiple gateway VNIs (150 and 350) under VTEP 1:

```
ACOS(config)# overlay-tunnel vtep 1
ACOS(config-overlay-tunnel:1)# encap nvgre
ACOS(config-overlay-tunnel:1)# local-ip-address 90.1.1.1
ACOS(config-overlay-tunnel:1-src-vtep:90...)# vni 200
partition px lif 4
ACOS(config-overlay-tunnel:1-src-vtep:90...)# vni 150
partition p1 lif 2 gateway
ACOS(config-overlay-tunnel:1-src-vtep:90...)# vni 350
partition p1 lif 3 gateway
ACOS(config-overlay-tunnel:1-src-vtep:90...)# vni 100
partition p1 lif 2
ACOS(config-overlay-tunnel:1-src-vtep:90...)# vni 300
partition p1 lif 3
ACOS(config-overlay-tunnel:1-src-vtep:90...)# exit
ACOS(config-overlay-tunnel:1)# remote-ip-address 100.1.1.2
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# encap nvgre
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# vni 100
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# vni 300
ACOS(config-overlay-tunnel:1-dst-vtep:10...)# exit
```

```
ACOS(config-overlay-tunnel:1)# remote-ip-address 100.1.1.3
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# encap nvgre
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# vni 100
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# vni 300
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# exit
ACOS(config-overlay-tunnel:1)# remote-ip-address 100.1.1.5
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# encap nvgre
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# vni 200
ACOS(config-overlay-tunnel:1-dst-vtep:100...)# exit
ACOS(config-overlay-tunnel:1)# host 80.1.1.11 AABB.CCDD.EEFF
vni 100 destination-vtep 100.1.1.3
ACOS(config-overlay-tunnel:1)# host 90.1.1.11 AAAA.BBBB.CCCC
vni 300 destination-vtep 100.1.1.2
```

overlay-tunnel options

Description Configures some of the system and packet behavior related to the tunnel configuration. This is a top-level command to begin the configuration of the overlay tunnel.

Syntax

```
[no] overlay-tunnel options
{
   fragmentation-mode-inner |
   gateway-mac mac-address |
   ip-dscp-preserve |
   nvgre-disable-flow-id |
   nvgre-key-mode-lower24 |
   src-port-range |
   tcp-mss-adjust-disable |
   vxlan-dest-port port |
}
```

NOTE: The **options** parameter and sub-parameters are only available in the shared partition.

Parameter	Description
fragmentation-mode-inner	Enable the inner fragmentation.
gateway-mac	Configures the MAC address for the gateway

Parameter	Description
mac-address	segment ID; this is mostly used with NVGRE in conjunction with the SCVMM. When configured, the ACOS device accepts all packets coming in with this MAC address. Outgoing packets, however use the corresponding LIF/VE MAC address. For more information about configuring a gateway, see the vni command.
vxlan-dest-port *port*	Specifies the port number (1-65535) on which you want your ACOS device to send and receive VXLAN traffic. The default port number is 4789.
ip-dscp-preserve	By default, the differentiated services code point (DSCP) value in the outer IP header for packets that are being tunnelled is set to the lowest priority. This optional command, when issued in the VTEP/underlay partition, copies the DSCP value from the inner IP header to the outer IP header for all overlay IP packets.
nvgre-disable-flow-id	The NVGRE header contains an 8 bit flow-id field that can be used to pass the entropy of the overlay flow that is being tunnelled across. The ACOS device will compute the entropy and pass it by default so that intermediate underlay routers/switches can make use of it for better link or ECMP load distribution. This optional command disables the flow-id computation for NVGRE and sets the flow-id to zero (0).
nvgre-key-mode-lower24	This optional command causes the lower 24-bits

Parameter	Description
	of the key field to be treated as the VSID. By default, only the upper 24 bits of the key field are treated as VSID (conforming to the NVGRE specification). Having this option allows for interoperability with varying implementations.
src-port-range	See src-port-range.
tcp-mss-adjust-disable	VXLAN and NVGRE tunneled packets get an additional header (50 bytes for VXLAN and 42 bytes for NVGRE) for IPv4 added. This addition can result in additional fragmentation of the packet if the exchanged maximum segment size (MSS) is not aware of this addition. The ACOS device will automatically adjust the MSS exchanged for TCP flows to take into account this header. Use this option to disable this automatic adjustment for Layer 4 TCP traffic.

Default N/A

Mode Configuration mode.

Usage If the ACOS device is a member of an aVCS virtual chassis, use the **device-context** command to specify the device in the chassis to which this command must apply.

Example The following example configures a VTEP with the ID of 1.

```
ACOS(config)# overlay-tunnel vtep 1
```

Example The following example removes a tunnel configuration (you are prompted to confirm the command).

```
ACOS(config)# no overlay-tunnel vtep 1
This command will delete the entire overlay-tunnel and related
sub-configuration. Proceed with deleting it? [yes/no] yes
ACOS(config)#
```

Related Commands:

- show running-config overlay-tunnel

src-port-range

Description Configures the layer-4 (UDP) source port range globally for VXLAN overlay tunnels.

Syntax

```
[no] overlay-tunnel option {src-port-range min-port num max-port num}
```

Parameter	Description
min-port *num*	Specify the minimum port number. The range can be from 1-65535.
max-port *num*	Specify the maximum port number. The range can be from 1-65535.

Default N/A

Mode Overlay Tunnel Options mode.

Usage ACOS selects the VXLAN UDP source (SRC) ports based on the following conditions:

- If the source port is not configured globally, then the minimum source port defaults to 1 and the maximum to 65535.
- If you do not configure a VTEP with a SRC port range, the VTEP uses the global SRC port range configured.
- Changing a VTEP SRC port range takes effect immediately, removing existing sessions in the VTEP and changes the VTEP to use the new SRC port range.
- If you change the global VXLAN UDP SRC port range, then existing VTEPs do not inherit the new SRC port range; only new VTEPs configured after the change will inherit the new SRC port range to prevent disruptions to existing VTEP sessions.

NOTE: For all existing VTEPs to use a configured global UDP SRC port range, save the configuration using the **write memory** command and reboot the device using the **reload** or **reboot** commands.

Example The following example configures the source port range globally.

```
ACOS(config)# overlay-tunnel options src-port-range min-port
1000 max-port 2000
```

Related Commands:

- src-port-range under VTEP

Show Commands

show interfaces brief

Description Shows the output of configured logical interface ports. The LIF ports will only appear in the overlay partition where the LIF is configured.

Syntax

```
show interfaces brief
```

Default N/A

Mode Enable mode.

Example The following output displays a summarized view of the interfaces configured on a device.

```
ACOS# show interfaces brief
Port    Link    Dupl    Speed   Trunk   Vlan    MAC IP Address
IPs Name
-------------------------------------------------------------
--------------
mgmt    Up      Full    100     N/A     N/A     000d.480a.6666
192.168.213.205/24                      1
1       Up      Full    1000    None    Tag     000d.480a.6665
0.0.0.0/0
2       Up      Full    100     None    Tag     000d.480a.6664
0.0.0.0/0                       0
3       Disb    None    None    None    1       000d.480a.6663
0.0.0.0/0                       0
4       Up      Full    1000    None    1       000d.480a.6662
0.0.0.0/0                       0
```

```
5       Up      Full    100     None    Tag     000d.480a.6661
0.0.0.0/0                       0
6       Up      Full    100     None    Tag     000d.480a.6660
0.0.0.0/0                       0
7       Disb    None    None    None    1       000d.480a.665f
0.0.0.0/0                       0
8       Disb    None    None    None    1       000d.480a.665e
0.0.0.0/0                       0
9       Disb    None    None    None    1       000d.480a.665d
0.0.0.0/0                       0
10      Disb    None    None    None    1       000d.480a.665c
0.0.0.0/0                       0
ve100   Up      N/A     N/A     N/A     100     000d.480a.6665
100.1.1.2/24                    1
ve120   Up      N/A     N/A     N/A     120     000d.480a.6665
120.2.1.1/24                    1
ve140   Up      N/A     N/A     N/A     140     000d.480a.6665
140.1.1.12/24                   1
ve160   Up      N/A     N/A     N/A     160     000d.480a.6665
160.1.1.12/24                   1
lif1    Up      N/A     N/A     N/A     1       000d.480a.6665
80.1.1.2/24                     1
```

The information in **bold** shows the logical interface.

show interfaces lif

Description Displays the logical tunnel interface details.

Syntax

```
show interfaces lif lif_num
```

Mode Enable mode

Example The following example shows sample output for this command:

```
ACOS# show interfaces lif 1
lif 1 is up, line protocol is up
Logical interface Lif, Address is 3eed.237d.7936
IPv6 address is 3001::2 Prefix 64 Type: unicast
IPv6 link-local address is fe80::3ced:23ff:fe7d:7936 Prefix 64
Type: Link-Local
```

```
GRE Encap, Local endpoint 20.20.20.2, Remote endpoint
20.20.20.1
IP MTU is 1500 bytes
131231 packets input 4986778 bytes
Received 0 broadcasts, Received 0 multicasts, Received 131231
unicasts
5 packets output 750 bytes
Transmitted 0 broadcasts, Transmitted 0 multicasts,
Transmitted 5 unicasts
```

show overlay-tunnel

Description Displays the overlay tunnel information.

Syntax

```
show overlay-tunnel { encap-table | vtep [ vtep-id |
statistics ] }
```

Parameter	Description
encap-table	Displays the IP address of encapsulated endpoints in the overlay tunnel.
vtep [vtep-id | statistics]	Displays the overlay-tunnel VTEP statistics.

Mode Enable mode.

Example The following example shows a sample output **show overlay-tunnel encap-table** command.

```
ACOS(config)# show overlay-tunnel encap-table
IP encap endpoints
------------------
Local endpoint Remote endpoint Encap type Static Age Vtep ID
LIF
------------------------------------------------------------------
------
2.2.2.1        2.2.1.1         IP-ENCAP    YES    0    2
test
3.3.3.1        3.3.3.2         VXLAN       YES    0    30
11.11.11.1     11.11.11.2      GRE         YES    0    3
5
1.1.1.1        1.1.1.2         IP-ENCAP    YES    0    1
6
```

The following table describes the fields in the command output.

Field	Description
Local endpoint	Source IP address of the tunnel endpoint.
Remote endpoint	Destination IP address of the tunnel endpoint.
Encap type	Types of encapsulation: • GRE • IP-Encap • NVGRE • VXLAN
Static	Indicates whether the entry is static.
Age	Number of seconds since the entry was last used in dynamic entries.
Vtep ID	ID of the virtual tunnel endpoint (VTEP).
LIF	Logical interface name that holds the tunnel endpoint.

Example The following example shows a sample output **show overlay-tunnel vtep statistics** command.

```
ACOS(config)# show overlay-tunnel vtep statistics
VTEP 1 Counters
Fragmented Pkts          0
Arp Reqs Sent            0
lif invalid: Drop Rx     0
lif not UP: Drop Rx      0
Unhandled Pkts: Drop Rx  0
In Total Pkts            0
In UCast Pkts            0
In BCast Pkts            0
In MCast Pkts            0
In Dropped Pkts          0
Cfg Error: Drop Pkt      0
In Encap Mismatch Pkts   0
In Bad v4 Inner len Pkts0
Reassembled Pkts         0
Host =&gt; VTEP Learned  0
lif invalid: Drop Tx     0
Encap unknown: Drop Tx   0
Unhandled Pkts: Drop Tx  0
Out Total Pkts           0
Out Ucast Pkts           0
Out BCast Pkts           0
Out MCast Pkts           0
Out Dropped Pkts         0
Out Flooded Pkts         2
In Bad Inner Chksum Pkts0
In Bad v6 Inner len Pkts0
```

show running-config overlay-mgmt-info

Description View information used by the SCVMM plugin to configure a connection string on the ACOS device.

Syntax

```
show running-config overlay-mgmt-info
```

Mode Enable mode

Example The following example shows sample output for this command:

```
ACOS(config)# show running-config overlay-mgmt-info
!Section configuration: 77 bytes
!
overlay-mgmt-info nvgre a10networks
!
overlay-mgmt-info scvmm a10Thunder
!
!
end
```

Related Commands:

- overlay-mgmt-info

show running-config overlay-tunnel

Description Displays the running configuration for the overlay tunnel. If no VTEP is specified, the configuration for all configured source VTEPs in the partition are displayed.

Syntax `show running-config overlay-tunnel { options | vtep vtep-id }`

Parameter	Description
`options`	Show partition-specific overlay tunnel configuration.
vtep *vtep-id*	Display the configuration for the specified VTEPs.

Mode Enable mode.

Example The following example shows sample output for this command:

```
ACOS(config)# show running-config overlay-tunnel
!
overlay-tunnel vtep 1
 encap vxlan
  local-ip-address 100.1.1.2
```

```
   vni 100 partition p1 lif 2
  remote-ip-address 90.1.1.1
   encap vxlan
   vni 100
!
```

Related Commands:

- overlay-tunnel options

show statistics interface

Description This command is extended so that you can specify a logical interface as well as an ethernet interface.

Syntax

```
show statistics interface lif lif-num
```

Replace *lif-num* with the logical interface number.

Default N/A

Mode Enable mode.

Example The following example shows sample output for this command:

```
ACOS# show statistics interface lif 1
Port     Link  Dupl Speed     IsTagged  MAC Address    IP
Address
-----------------------------------------------------------------
---------------
lif 1    Up    NA   NA        Untagged  3EED.237D.7936 0.0.0.0

-----------------------------------
Lif 1 Counters:
-----------------------------------
InPkts                  131245
OutPkts                 5
InOctets                4987310
OutOctets               750
InBroadcastPkts         0
OutBroadcastPkts        0
InMulticastPkts         0
```

```
OutMulticastPkts         0
InBadPkts                0
OutBadPkts               0
InDisDroppedPkts         0
OutDisDroppedPkts        0
InGreKeyMisPkts          0
```

show vlans

Description Shows the configured logical interface ports along with ethernet ports.

Syntax

```
show vlans [num]
```

Replace *num* with the vlan number (2-4094).

Default N/A

Mode Enable mode.

Example The following example shows sample output for this command:

```
ACOS# show vlans
Total VLANs: 2
VLAN 1, Name [DEFAULT VLAN]:
Untagged Ethernet Ports:    1   2   3   4   5   6   7   8
  Tagged Ethernet Ports:   None

VLAN 100, Name [None]:
Untagged Ethernet Ports:   None
  Tagged Ethernet Ports:   None
 Untagged Logical Ports:   lif2

VLAN 200, Name [None]:
Untagged Ethernet Ports:   None
  Tagged Ethernet Ports:   10
       Router Interface:   ve 200
```

The line in bold shows the logical interface in the output.

Application Access Management

Application Access Management (AAM) optimizes Authentication, Authorization, and Accounting (AAA) for client-server traffic. It centralizes control for managing access, eliminates the need to manage individual services on multiple servers, and simplifies login through single sign-on (SSO) technology. By providing a consistent way to access services, AAM ensures a highly available and scalable means to ensure the proper authentication of client-server traffic.

This reference lists the CLI configuration and show commands that apply specifically to AAM.

Configuration Commands

aam

Description Configure AAM related configuration, such as configuring AAM AAA policies, AAM authentication related settings, and AAM authorization related settings.

Syntax

```
[no] aam
```

Parameter	Description
`aaa-policy`	Configure AAM AAA policy configuration.
`authentication`	Configure AAM authentication related configuration.
`authorization`	Configure AAM authorization related configuration.

Default None

Mode Configuration Mode

aam authentication

Description Configure AAM authentication settings.

Syntax `[no] aam authentication`

Parameter	Description
account	Configure authentication account.
global	Display global AAM authentication statistics.
log	Configure authentication log.
logon	Configure authentication logon.
portal	Configure the authentication portal.
relay	Configure authentication relay.
saml	Configure AAM SAML-related configuration.
server	Configure the authentication server.
service-group	Configure the authentication service group.
template	Configure authentication template.

Default None

Mode Configuration Mode

aam authentication account

Description Configure AAM authentication accounts.

Syntax `[no] aam authentication account`

Parameter	Description
kerberos-spn	Configure an AD domain account associated with a SPN.
sampling-enable	Enable baselining.

Default None

Mode Configuration Mode

Usage See the "Enabling Baselining and Rate Calculation" topic of the *Command Line Interface Reference* for an explanation of baselining. The `show counters-baselining` command displays the enabled counters.

aam authentication account kerberos-spn

Description Configure an Active Directory domain account with a Kerberos SPN and specify account credentials.

Syntax

```
[no] aam authentication account kerberos-spn profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] **account** *account-name-string*	Admin account name required to logonto the Active Directory server.
[no] **password** *string*	Password required for logging onto the Active Directory server.
[no] **realm** *realm-string*	URL of the host realm for the Active Directory server.
[no] **service-principal-name** *string*	Name of the account object used for the authentication service instance.
[no] **user-tag** *string*	Customized tag.

Default None

Mode Configuration Mode

aam authentication account sampling-enable

Description Enable baselining.

Syntax

```
[no]authentication account sampling-enable
```

Parameter	Description
all	Include all responses.
request-normal	Configure the total normal request.
request-dropped	Configure the total dropped request.
response-success	Configure the total success response.
response-failure	Configure the total failure response.
response-error	Configure the total error response.
response-timeout	Configure the total timeout response.
response-other	Configure the total other response.

Default None

Mode Configuration Mode

Usage See the "Enabling Baselining and Rate Calculation" topic of the *Command Line Interface Reference* for an explanation of baselining.

The `show counters-baselining` command displays the enabled counters.

aam authentication global

Description Display global AAM authentication statistics.

Syntax `[no] aam authentication global`

Default None

Mode Configuration Mode

aam authentication jwt

Description Configures JWT template for JWT issuance

Syntax `aam authentication jwt <template-name>`

Command	Description
[no]	Specifies JWT issuer ("**iss**") claim value.

Command	Description
issuer	
[no] action *action*	Specifies JWT issuance action (default is **relay**). • **orelay (default):** JWT relays to back-end application server like other AAM relay feature. • **oredirect:** JWT is redirected to specific URI by appending to URI parameter.
[no] signature-secret *secret*	Specifies the secret to sign the JWT signature.
[no] token-lifetime *seconds*	Specifies the valid duration of the JWT when it is generated.
[no] client-error-resp-code *400-499*	Specifies the HTTP response code to return when JWT validation fails. You can configure any value between 400 and 499. This setting determines the HTTP status code sent to the client when the JWT is expired, invalid, or missing. **NOTE:** By default, the system returns 401 (Unauthorized) for AAM authentication flows and 407 (Proxy Authentication Required) for Explicit Proxy or Proxy Chaining flows.

Example The following example shows the how to configure the client error response code to return HTTP 402 when JWT validation fails:

```
ACOS(config-jwt-authz:j1)# client-error-resp-code 402
```

aam authentication log

Description Configure AAM authentication logs.

Syntax `[no] aam authentication log`

Parameter	Description
`enable`	Enable authentication logs.
`facility`	Specify the facility on syslog server to send authentication logs. The default is local0.
`format`	Set the log format

Syntax `[no] aam authentication log format`

Parameter	Description
`syslog`	Syslog format, which is default.
`cef`	Common Events Format

Default None

Mode Configuration Mode

aam authentication log enable

Description Enable collection of authentication logs for generated authentication data.

Syntax `[no] aam authentication log enable`

This command changes the CLI to the configuration level for the profile. In the current release, no commands specific to this type of profile are available.

Default None

Mode Configuration Mode

aam authentication log facility

Description Specify the location on the syslog server to send authentication logs.

Syntax `[no] aam authentication log facility facility-name`

Default The default facility is local 0.

Mode Configuration Mode

aam authentication logon

Description Configure AAM authentication logon.

Syntax `[no] aam authentication logon`

Parameter	Description
form-based	Configure form-based authentication logon.
http-authenticate	Configure HTTP-authenticate logon.

Default None

Mode Configure Mode

aam authentication logon form-based

Description Configures an authentication logon profile for form-based logon.

Syntax `[no] aam authentication logon form-based` *profile-name*

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] action-url *url-string*	URL for the POST action to be performed by the client browser after the end-user enters their credentials. Use this option if the URL is not the same as the URL for the page that contains the form. Use the following format: **/***url-string*
[no] authz-failure-message *string*	Specify authorization failure message shown in logon page.
[no] captcha-variable <captcha_var_name>	Specify the variable name of CAPTCHA token used in the logon form.

Parameter	Description
[no] challenge-variable	Specify a challenge variable name on the form submission.
[**no**] **changepassword-url** *string*	URL for the POST action to be performed by the client browser after the end-user enters their expired and new credentials.

[**no**] **csp-support {none | self | sepcificURI}**	Inserts the HTTP Content-Security-Policy and X-Frame-Options headers during the AAM authentication to enhance the security. The following options are available:
	• **none**— Sets CSP frame-ancestors to none (also X-Frame-Options deny).
	• **self**—Sets CSP frame-ancestors to self (also X-Frame-Options same-origin).
	• **specificURI**—Sets customized CSP frame-ancestors (maximum 2 URIs can be set).
	Examples for URI,
	`https://a.example.com`
	`https://b.example.com`

[**no**] **disable-change-password-link** *string*	The command disables the display of the change password link on the logon page. The change password link will not be displayed even if the back-end authentication server supports it.
[**no**] **hsts-support timeout** *<second>*	Inserts the HTTP Strict-Transport-Security header during the AAM authentication to enhance security. Sets the HSTS policy expiry timeout in seconds. The timeout value can be

Parameter	Description
	between 0-315360000 seconds. If the timeout is set to 0 it disables the HSTS policy.
[no] **login-failure-message** *string*	Message to display to an end-user if their login attempts fails. The message string is included in the logon form resent by AAM to the end-user.
[no] **new-pin-variable** *string*	Specify the new-pin variable name used when the form is submitted.
[no] **next-token-variable** *string*	Specify the next-token variable name used when the form is submitted.
[no] **notifychangepassword-change-url string**	URL for the POST action to be performed by the client browser after the end-user saves the new credentials.
[no] **notifychangepassword-continue-url string**	URL for the POST action to be performed by the client browser after the end-user confirms the password change.
[no] **passcode-variable** *string*	Name of the data field for the passcode entered into the logon form by the end-user.
[no] **password-variable** *string*	Name of the data field for the password entered into the logon form by the end-user.
[no] **portal default-portal** or [no] **portal** *name* **logon** *name* **failpage** *name* **changepasswordpage** *name*	Configure a logon portal for form-based logon. If you are defining a custom portal, the following options are available: • **logon**—Name of the page that users will see when the successfully logon to the portal. • **failpage**—Name of the page that

Parameter	Description
{**new-pin-page** *name* **next-token-page** *name* | **challenge-page** *name*}	users will see if they unsuccessfully attempt to logon. • **changepasswordpage**—Name of the page allowing users to change their password. • **new-pin-page**—Name of the page where users can define a new PIN for RSA-RADIUS authentication. • **next-token-page**—Name of the page where users can define the next token for RSA-RADIUS authentication. • **challenge-page** -Specify challenge page name (uri = chall.html) for RSA-RADIUS
[**no**] **retry** *num*	Number of times ACOS will resend the authentication request to the client, to allow the end-user to re-enter their credentials. You can specify 1-32. The default is 3. account-lock - ACOS locks the user account after the user exceeds the configured failed logon attempts.
[**no**] **retry** *num* *account-lock*	The time an account remains locked after the ACOS detects no password retry failures from the user. duration - The time (in seconds) after which the account will be unlocked. The default is 60 seconds.
[**no**] **user-tag** *string*	Customized user tag.
[**no**] **username-variable** *string*	Name of the data field for the username entered into the logon form by the end-

Parameter	Description
	user.
[no] **changepassword-username-variable** *string*	Name of the data field for the username entered into the change-password form by the end-user.
[no] **changepassword-old-password-variable** *string*	Name of the data field for the old password entered into the change-password form by the end-user.
[no] **changepassword-new-password-variable** *string*	Name of the data field for the new password entered into the change-password form by the end-user.
[no] **changepassword-password-confirm-variable** *string*	Name of the data field for the confirmed new password entered into the change-password form by the end-user.

Default There are no default authentication-logon profiles. When you create one for form-based logon, the profile has no default values.

Mode Configuration Mode

aam authentication captcha

Description Configuration of AAM authentication captcha.

Syntax

```
aam authentication captcha <name>
```

Parameter	Description
[no] secret-key <key>	Server secret key used when verifying the CAPTCHA token.
[no] url <api_url>	API URL used for CAPTCHA verification. The scheme should be HTTP or HTTPS.
[no] method {POST | GET}	HTTP method that API URL uses; default is POST. This option will be always displayed on

Parameter	Description
	CLI.
`timeout {1..255}`	Timeout value when waiting for response. The range is from 1 to 255 seconds, default is 10 seconds.
`secret-key-param-name <param_name>`	Parameter name of secret-key used in CAPTCHA API verification.
`token-param-name <param_name>`	Parameter name of token used in CAPTCHA API verification.
`resp-result-field-name <field_name>`	Response result field name.
`resp-error-msg-field-name <field_name>`	Field name of error message in the CAPTCHA JSON response
`send-client-ip param-name <field_name>`	Send the client IP address in CAPTCHA challenge and also set the parameter name used in CAPTCHA API

aam authentication logon http-authenticate

Description Configure an authentication-logon profile for HTTP-based logon.

Syntax

```
[no] aam authentication logon http-authenticate profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] auth-method { basic { challenge-response-form *name*	Specify the type of authentication logon mechanisms. • **basic challenge-response-form**—Define a challenge-response form for RSA-RADIUS authentication. ◦ `challenge-page` -Specify challenge page name (uri = chall.html) for RSA-RADIUS

Parameter	Description
challenge-page *name* challenge-variable *name* | **new-pin-page** *name* **next-token-page** *name* **new-pin-variable** *name* **next-token-variable** *name* | **enable** | **realm** *name*} | **negotiate enable** | }	◦ `challenge-variable`-Specify challenge variable name • **basic enable**—Enables a basic authentication logon. • **basic realm**—Specify a realm for basic logon. • **negotiate enable**—Enables a Kerberos-based SPNEGO protocol for the authentication logon.
[**no**] **hsts-support timeout** *<second>*	Inserts the HTTP Strict-Transport-Security header during the AAM authentication to enhance security. Sets the HSTS policy expiry timeout in seconds. The timeout value can be between 0-315360000 seconds. If the timeout is set to 0 it disables the HSTS policy.
[**no**] **packet-capture-tem-**	Specify name of the packet capture template to bind with this object.

Parameter	Description
plate *string*	
[**no**] **retry** *num*	Number of times ACOS will resend the authentication request to the client, to allow the end-user to re-enter their credentials. You can specify 1-32. The default is 3.
[**no**] **sampling-enable** *num*	Enables baselining.

Default There are no default authentication-logon profiles. When you create one for basic HTTP logon, the default retry value is 3.

Mode Configuration Mode

aam authentication portal

Description Configure an authentication portal

Syntax

```
[no] aam authentication portal
```

aam authentication portal default-portal

Description Configure a default authentication portal. This command changes the CLI to the configuration level for the profile, where the following commands are available.

Syntax

```
[no] aam authentication portal default-portal
```

Parameter	Description
change-password	Change the password page configuration. The following commands are available after you enter **change-password**: • **action-url**– Specify the form action URL in the default change password page (1-63 characters). The default is `/change.fo`.

Parameter	Description
	• **background** {**color** *color* | **file** *name*}— Configure the background on the default change password page. You can specify a color, either by name or hex value, or a file to use for the background. The default is `a10bg.gif`. • **confirm-password** — Configure the confirm password text on the default change password page. Specify at least one of the following: • **color** *color* - name or hex value for the desired font color. • **font** *font-name* - font type to use for the text. Type **font ?** to see the list of available fonts. • **size** *size* - size of the font (1-7). • **text** *string* - text you want to use on the page (1-63 characters). • **confirm-password-var** - Configure the confirm password variable name on the default change password page (1-63 characters). The default is `cp_cfm_pwd`. • **new-password** - Configure the new password text on the default change password page. The sub-options are the same as **confirm-password** (above). • **new-password-var** - Configure the new password variable name on the default change password page (1-63 characters). The default is `cp_new_pwd`. • **old-password** - Configure the old password text on the default change password page.

Parameter	Description
	The sub-options are the same as **confirm-password** (above). • **old-password-var** - Configure the old password variable name on the default change password page (1-63 characters). The default is `cp_old_pwd`. • **reset-text** - Configure the text you want to appear on the Reset button on the default change password page (1-63 characters). The default is "Reset." • **submit-text** - Configure the text you want to appear on the Submit button on the default change password page (1-63 characters). The default is "Submit." • **title** - Configure the title on the default change password page. The sub-options are the same as **confirm-password** (above). • **username**- Configure the username text on the default change password page. The sub-options are the same as **confirm-password** (above). • **username-var** - Configure the username variable name on the default change password page (1-63 characters). The default is `cp_usr`.
logo *filename* [**height** *num*] [**width** *num*]	Specify the name of the image file you want to use for the logo (1-63 characters), and use a .BMP .GIF .JPG, or .PNG file. You can also specify the **height** (50-400 pixels) and/or **width** (50-400 pixels) of the image.
logon	Configure the login page for the default portal. The following commands are available after you

Parameter	Description
	enter **logon**: • **action-url**– Specify the form action URL (1-63 characters). The default is /logon.fo. • **background** {**color** *color* | **file** *name*}– Configure the background on the logon page. You can specify a color, either by name or hex value, or a use a .BMP .GIF .JPG, or .PNG file.to use for the background. The default is def_bg.gif. When using an image file, the the image can be tiled, stretched, or fitted across the page. • **enable-passcode** - Enable the Passcode field on the logon page. • **fail-msg** - Configure the message users will see if their logon attempt fails (1-63 characters). Specify at least one of the following: ◦ **color** *color* - name or hex value for the desired font color. ◦ **font** *font-name* - font type to use for the text. Type **font ?** to see the list of available fonts. ◦ **size** *size* - size of the font (1-7). ◦ **text***string* - text you want to use (1-63 characters). The default is “Invalid username or password. Please try again.” • **passcode** - Configure the text you want to use for the Passcode field. The sub-options are the same as **fail-msg** (above). The default is “Passcode.”

Parameter	Description
	• **passcode-var** - Configure the passcode variable name on the logon page (1-63 characters). The default is `passcode`. • **password** - Configure the text you want to use for the Password field. The sub-options are the same as **fail-msg** (above). The default is "Password." • **password-var** - Configure the password variable name on the logon page (1-63 characters). The default is `pwd`. • **submit-text** - Configure the text you want to appear on the Submit button (1-63 characters). The default is "Submit." • **username**- Configure the text you want to use for the Username field on the logon page. The sub-options are the same as **fail-msg** (above). The default text is "username." • **username-var** - Configure the username variable name on the logon page (1-63 characters). The default is `user`.
logon-fail	Configure the login failed page for the default portal. The following commands are available after you enter **logon-fail**: • **background** {**color** *color* | **file** *name*}— Configure the background on the logon page. You can specify a color, either by name or hex value, or a file to use for the background. The default is `a10bg.gif`. • **background** {**color** *color* | **file** *name*}— Configure the background on the logon page. You can specify a color, either by name or hex value, or a file to use for the background. The

Parameter	Description
	default is `a10bg.gif`. ◦ **`color`** *`color`* - name or hex value for the desired font color. ◦ **`font`** *`font-name`* - font type to use for the text. Type **`font ?`** to see the list of available fonts. ◦ **`size`** *`size`* - size of the font (1-7). ◦ **`text`** *`string`* - text you want to use (1-63 characters). The default is “Login failed!” • **`title`** - Configure the title on the default change password page. The sub-options are the same as **`fail-msg`** (above), except that there is no default text string.
notify-change-password	Password change notification page configuration. The following commands are available after you enter **`notify-change-password:`** background {**`color`** *`color`* | **`file`** *`name`*}— Configure the background on the default change password notification page. You can specify a color, either by name or hex value, or a file to use for the background. The default is `a10bg.gif`.- change-text - Configure the change button text on the default password notification page. The default is Change. change-url - Configure the change password action URL on the default change password notification page. The default is /notify_ change.fo. confirm-password - Configure the confirm

Parameter	Description
	password text on the default change password notification page. Specify at least one of the following: • **color** *color* - name or hex value for the desired font color. • **font** *font-name* - font type to use for the text. Type **font ?** to see the list of available fonts. • **size** *size* - size of the font (1-7). • **text** *string* - text you want to use on the page (1-63 characters). • confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is `cp_cfm_pwd` • confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is • confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is `cp_cfm_pwd` • confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is `cp_cfm_pwd` • confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is `cp_cfm_pwd`

Parameter	Description
	• old-password - Configure the old password text on the default change password notification page. The sub-options are the same as **confirm-password** (above) • old-password - Configure the old password text on the default change password notification page. The sub-options are the same as **confirm-password** (above) • old-password - Configure the old password text on the default change password notification page. The sub-options are the same as **confirm-password** (above) • old-password - Configure the old password text on the default change password notification page. The sub-options are the same as **confirm-password** (above)
enable-CAPTCHA type {reCAPTCHAv2-checkbox | reCAPTCHAv2-invisible | reCAPTCHAv3} site-key <key>	Enable Google `reCAPTCHA` in default-portal logon page and set the site-key. • **reCAPTCHA-theme {light | dark}**- The color theme of the widget. Default theme is light. This option is only available when using reCAPTCHAv2. • **reCAPTCHA-size {normal | compact}** - Size of the widget. The default size is normal. This option is only available when using reCAPTCHAv2. • **reCAPTCHA-size {normal | compact}** - Size of the widget. The default size is normal. This option is only available when using reCAPTCHAv2. • **reCAPTCHA-size {normal | compact}** - Size of the widget. The default size is normal. This option is only available when using reCAPTCHAv2.

Parameter	Description
	NOTE: According to Google limitation, the action string only accepts alphanumeric, '/', and '_'.

Mode Configuration mode

Example Enter portal configuration mode:

```
ACOS(config)# aam authentication portal default-portal
ACOS(config:default-portal)#
```

aam authentication relay

Description Configure authentication relay

Syntax

```
[no] aam authentication relay
```

Parameter	Description
form-based	Configure form-based authentication relay.
http-basic	Configure HTTP basic authentication relay.
kerberos	Configure Kerberos authentication relay.
ntml	Configure NTML authentication relay.
ws-federation	Configure WS-Federation authentication relay.

Default None

Mode Configuration Mode

aam authentication relay form-based

Description Configure an authentication relay profile for form-based authentication.

Syntax

```
[no] aam authentication relay form-based profile-name
```

This command changes the CLI to the configuration level for the profile, where the following sub-commands are available:

Sub-commands	Sub-command Description and Syntax
`[no] request-uri {equals | contains | starts-with | ends-with} uri`	Specifies the URI path of the authentication web page and enters the mode in which authentication web page options are configured. The following sub-commands are accessed under the **`request-uri`** command: • [no] `action-uri uri` - Specify the action-URI. • [no] `domain-variable domain-var` - Specify domain variable name • [no] `header cookie cookie-string` - Specify new header content in the POST packet by specifying a new cookie in POST packet. • [no] `max-packet-collect-size bytes` - Specifies the number of bytes reserved for response packet collection in bytes. The default is 1MByte. • [no] `other-variables other-var` - Specify other variables (n1=v1&n2=v2) in form relay. • [no] `password-variable pw-var` -

Sub-commands	Sub-command Description and Syntax
	Specify password variable name. • [no] `user-variable` *`username-var`* - Specify the username variable name.
`[no] sampling-enable [all] [request] [invalid_srv_rsp] [post_fail] [invalid_cred] [bad_req] [not_fnd] [error] [other_error]`	Enables baselining the specified relayed message counters. See the "Enabling Baselining and Rate Calculation" topic in the *Command Line Interface Reference* for an explanation of baselining. • `all` - all message types. • `request` - requests • `invalid_srv_rsp` - "Invalid Server" responses • `post_fail` - "Post Failed" responses • `invalid_cred` - "Invalid Credentials" responses • `bad_req` - "Bad Found" responses • `not_fnd` - "Internal Server Error" responses • `error` - "Bad Request" responses • `other_error` - "Other Error" responses

Default None

Mode Form-Based Relay Configuration Mode

Usage When the user configures form-based relay, the name of variables are set. If the application server replies with a form-based web page for authentication (ACOS knows the page is for authentication by checking some keywords), ACOS uses the information in Auth-relay and auth_ info to reply to the application server and complete the authentication.

The user can also use the multiple authentication web pages in one VIP. In this case, the user can configure multiple settings for different web pages. Every setting has a different request-url parameter as its index, and each setting is responsible for its corresponding web page.

aam authentication relay http-basic

Description Configure an authentication relay profile for basic HTTP authentication.

Syntax

```
[no] aam authentication relay http-basic profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available:

Parameter	Description
domain *domain-name*	Specify the user domain.
domain-format {**user-principal-name** | **down-level-logon-name**}	Specify the format to use for appending the domain to the credential: • **user-principal-name** - Append the domain using the User Principal Name format (for example: *user@domain*). • **down-level-logon-name** - Append the domain using the Down Level Logon Name format (for example: *domain\user*). The default is **down-level-logon-name**.

Default None

Mode Configuration Mode

aam authentication relay kerberos

Description Configure an authentication-relay profile for Kerberos authentication.

Syntax

```
[no] aam authentication relay kerberos profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] kerberos-account *name* [...]	Kerberos admin account name required to logonto the KDC.
[no] kerberos-kdc {*hostname* | *ipaddr*}	Hostname or IP address of the KDC.
[no] kerberos-kdc-service-group {*auth_service_group*}	Name of the service group for multiple KDC servers configured in AAM (under authentication server).
[no] kerberos-realm *realm-string*	Name of the Kerberos realm secured by the AAA servers.
[no] password *string*	Password required for logging onto the KDC.
[no] port *port-num*	Protocol port number on which the KDC listens for requests.

Parameter	Description
	The default port is 88.
[no] **timeout** *seconds*	Maximum number of seconds ACOS waits for the Kerberos server to respond to a request. If a request times out, ACOS aborts that request. You can specify 1-255 seconds. The default timeout is 10 seconds.

Default There are no default authentication-relay profiles. When you create one, it has the default values described in the table above.

Mode Configuration Mode

aam authentication relay saml

Description Configure an authentication relay profile for SAML authentication

Syntax

```
[no] aam authentication relay saml <name>
```

Parameter	Description
[no]relay-acs-uri *<URI>*	Specify the backend server assertion consuming service URI
[no]server-login-uri *<uri>*	Specify the URI to trigger the SAML relay.
[no] server-cookie-name *<name>*	Specify the cookie name that used by backend server for authenticated users. Then Thunder will trigger the relay when the cookie is missing.
relay-state value *<string>* | **request-uri | get-from-backend**	Specify how Thunder provide the RelayState when relay • value <string>: Specify a fixed string as the RelayState when relay • request-uri: Specify to use the (URL encoded) current request-uri as the RelayState

Parameter	Description
	• get-from-backend: Specify Thunder should try to get RelayState from backend server

Default None

Mode Configuration Mode

aam authentication relay ws-federation

Description Configure an authentication relay profile for ws-federation authentication.

Syntax

```
[no] aam authentication relay ws-federation profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available:

Parameter	Description
[no] application-server {**sharepoint** | **exchange-owa**}	Specify the type of application server: • **sharepoint** - Microsoft Sharepoint • **exchange-owa** - Microsoft Exchange The default is Microsoft **sharepoint**.
[no] **authentication-uri** *uri-name*	Specify WS-Federation relay URI. The default URI is `/_trust/`.

Default None

Mode Configuration Mode

aam authentication saml

Description Configure SAML-related settings.

Syntax

```
[no] aam authentication saml
```

Parameter	Description
identity-provider	Configure SAML authentication identity provider.
service-provider	Configure SAML authentication service provider.

Default None

Mode Configuration Mode

aam authentication saml identity-provider

Description Configure profile and specifications for the identity provider within Security Assertion Markup Language (SAML) for authentication.

Syntax

```
[no] aam authentication saml identity-provider name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available.

```
[no] metadata url
```

Replace *url* with the URL of the SAML identity provider's metadata file (1-63 characters)

Default None

Mode Configuration Mode

aam authentication saml service-provider

Description Configure profile and specifications for the service provider within Security Assertion Markup Language (SAML) for authentication.

Syntax

```
[no] aam authentication saml service-provider name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] SP-initiated-single-logout-service *location*	Decide the endpoint of SP-initiator Single Logout (SLO) service. Specify the location of the SP-initiator SLO (for example, /Logout).
[no] **acs-uri-bypass**	After user is authenticated, bypass requests with assertion-consuming-service location URI.
[no] **adfs-ws-federation enable**	Enable ADFS WS_Federation.
[no] **artifact-resolution-service index** *index-num* **location** *string* **binding soap**	The SAML service provider artifact resolution service configuration. Specify the index number of the artifact resolution service (0-5), and the location of the artifact resolution service (for example, /SAML/POST), and SOAP binding of the artifact resolution service.
[no] **assertion-consuming-service index** *index-num* **location** *string* **binding** {**artifact** | **paos** | **post**}	The SAML service provider assertion consuming service configuration. Specify the index number of the assertion consuming service (0-5), and the location of the assertion consuming service (for example, /SAML/POST), and the binding: • **artifact** - Artifact binding of the assertion consuming service. • **paos** - PAOS binding of the assertion consuming service. • **post** - POST binding of the assertion consuming service.
[no]**bad-request-**	Specify a URL to redirect.

Parameter	Description
redirect-url *Name*	You can specify a string of 1-127 characters.
[**no**] **certificate** *filename*	The SAML service provider certificate file (1-63 characters).
[**no**] **entity-id** *id*	The SAML service provider entity ID (1-63 characters).
[**no**] **metadata-export-service location** *uri* [**sign-xml**]	The SAML service provider metadata export service. The default location is `/A10SP_Metadata`. The **sign-xml** option signs the exported service provider metadata XML with service provider's certificate.
packet-capture-template	Specify a name for the packet capture template to be bind with this object. You can specify a string of 1-127 characters.
[no] **require-assertion-signed enable**	Require SAML assertion to be signed.
[**no**] **saml-request-signed disable**	Signing SAML requests (AuthnRequest or Artifact Resolve).
[**no**] **sampling-enable**	Enables baselining the specified message counters. See the “Enabling Baselining and Rate Calculation” topic in the *Command Line Interface Reference* for an explanation of baselining.
[**no**] **service-url** *url*	SAML service provider service URL (for example, `https://www.a10networks.com/saml.sso`).
[no] **signature-algorithm {SHA1 | SHA256}**	Specify SAML request signature algorithm

Parameter	Description
[no] **single-logout-service** {post | redirect | soap}	The SAML service provider single logout service configuration. Specify the location of the single logout service (for example, /SAML/POST), and the binding: • **post** - POST binding of the single logout service. • **redirect** - Redirect binding of the single logout service. • **soap** - SOAP binding of the single logout service.
[no] **soap-tls-certificate-validate**	Verify the IDP certificate when you establish the TLS connection to IDP for Artifact resolution.
[no] **username-attribute** *username*	Specify a username to identify and differentiate individual users within the database. You can specify a string of 1-63 characters.
user-tag *tag-name*	Customized user tag for SAML service provider. You can specify a string of 1-127 characters.

Default None

Mode Configuration Mode

aam authentication server

Description Configure AAM authentication servers.

Syntax `[no] aam authentication server`

Parameter	Description
idap	Configure a LDAP as the authentication server.
ocsp	Configure an OCSP server as the authentication server.
radius	Configure a RADIUS server as the authentication server.
windows	Configure a Microsoft Windows server as the authentication server.

Default None

Mode Configuration Mode

aam authentication server ldap

Description Configure an authentication-server profile for a Lightweight Directory Access Protocol (LDAP) server.

Syntax

```
[no] aam authentication server ldap profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available:

Parameter	Description
[no] **admin-dn** *string*	The Distinguished Name (DN) of the LDAP admin account that is required to access the server (1-127 characters).
[no] **admin-secret** *string*	Admin password (1-128 characters).
[no] auth-type	LDAP authentication server type (active directory or open LDAP).
[no] **base** *string*	LDAP server's search base (1-127 characters).
[no] **bind-with-dn**	DN must be used for LDAP binding.
[no] **default-**	Default domain for LDAP (1-63 characters).

Parameter	Description
domain *domain-name*	
[**no**] **derive-bind-dn username-attr** *attr-name*	Derive Distinguished Name for binding from server. Specify the attribute name of username (1-31 characters).
[**no**] **dn-attribute** *attr-name*	Specify Distinguished Name attribute (1-31 characters). The default is **CN**.
[**no**] **health-check** *mon-name*	Check the server's health check status. Specify the name of an existing health check monitor (1-63 characters).
[**no**] **health-check-disable**	Disable the configured health check configuration.
[**no**] **host** {*hostname* | *ipaddr*}	Hostname or IP address of the LDAP server.
[**no**] **port** *port-num*	Protocol port on which the server listens for LDAP traffic. The default port is 389.
[**no**] prompt-password-change-before-expiration	Prompt the user to change the password before the specified number of days prior to expiration
[**no**] **pwdmaxage** *seconds*	Maximum amount of time an end-user's password can be cached. You can specify 1-4294967295 seconds. This is not set by default.
[**no**] **protocol** *string*	The type of connection to used by ACOS when querying the LDAP directory server for user

Parameter	Description
	authentication. • ldap – Starts a plain text connection. • ldaps – Creates a SSL socket and LDAP messages are sent and received over it. • starttls - An existing insecure plain text connection is upgraded to a secure connection and the connection is encrypted using TLS.
[**no**] ca-cert	The trusted Certificate Authority (CA) certificate to be used for LDAP over SSL connections. **NOTE:** This command is available ONLY when the protocol is set to *ldaps* or *starttls*.
[**no**] **timeout** *seconds*	Maximum number of seconds ACOS waits for the LDAP server to respond to a request. If a request times out, ACOS aborts that request. You can specify 1-255 seconds. The default is 10 seconds.
[**no**] ldaps-conn-reuse-idle-timeout *seconds*	Maximum number of seconds an LDAP connection can remain idle before the connection is closed and removed from the LDAP connection pool. The default value is zero (0). Range: 0 - 86400 seconds

Default There are no default authentication-server profiles. When one is created, the default values are specified in the descriptions above.

Mode Configuration Mode

aam authentication server ocsp

Description Configure an authentication-server profile for an Online Certificate Status Protocol (OCSP) server.

Syntax

```
[no] aam authentication server ocsp profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available:

Parameter	Description
[no] **health-check** *mon-name*	Check the server's health check status. Specify the name of an existing health check monitor (1-63 characters).
[no] **health-check-disable**	Disable the configured health check configuration.
[no] **port-health-check** *mon-name*	Check the port's health check status. Specify the name of an existing health check monitor (1-63 characters).
[no] **port-health-check-disable**	Disable the configured port health check configuration.
[no] **responder-ca**	
[no] **responder-cert**	The trusted OCSP responder's certificate filename.
[no] **url** *url-string*	The OCSP server's address in the following format: **http://***host*[:*port*]**/)**

Default There are no default authentication-server profiles. When you create one for OCSP, it has no default values.

Mode Configuration Mode

aam authentication server radius

Description Configure an authentication-server profile for a RADIUS server.

Syntax

```
[no] aam authentication server radius profile-name
```

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] **accounting-port** *port-num*	Protocol port on which the server sends RADIUS accounting messages for authentication session creation and deletion. The default port is 1813.
[no] **auth-type** {**pap** | **mschapv2** | **mschapv2-pap**}	Specify the type of authentication: • **pap**–PAP authentication. It is selected by default. • **mschapv2**–MS-CHAPv2 authentication. • **mschapv2-pap**–Use MS-CHAPv2 first. If the server doesn't support MS-CHAPv2, the server tries for PAP.
[no] **health-check** *mon-name*	Check the server's health check status. Specify the name of an existing health check monitor (1-63 characters). This command is also available specifically for an accounting-port or port.
[no] **health-check-disable**	Disable the configured health check configuration. This command is also available specifically for an accounting-port or port.
[no] **host** {*hostname* | *ipaddr*}	Hostname or IP address of the RADIUS server.
[no] **interval** *seconds*	Maximum number of seconds ACOS will wait for a reply to a request before resending the request. You can specify 1-1024 seconds. The default interval is 3.
[no] **port** *port-num*	Protocol port on which the server listens for RADIUS traffic.

Parameter	Description
	The default port is 1812.
[no] **retry** *num*	Maximum number of times ACOS will send the same request before giving up. You can specify 1-32. The default retry is 5.
[no] **secret** *string*	Password, 1-128 characters, required by the RADIUS server for authentication requests.

Default There are no default authentication-server profiles. When you create one, it has the default values specified in the table above.

Mode Configuration Mode

aam authentication server windows

Description Configure an authentication-server profile for a Windows server for either Kerberos or Windows Integrated Authentication.

Syntax `[no] aam authentication server windows profile-name`

This command changes the CLI to the configuration level for the profile, where the following commands are available.

Parameter	Description
[no] **auth-protocol** *protocol*	Specifies an enabled authentication protocol. The user can choose among the following: • **kerberos-port** *value* –Specify the Kerberos port, default is 88. • **kerberos-validate-kdc** - Enable validation for the Kerberos KDC server port. • **health-check** *string*–Specify a previously configured health monitor for running health checks on the Kerberos KDC server port. • **health-check-disable**–Disable a configured

Parameter	Description
	health check for the Kerberos KDC server port. • **kerberos-password-change-port value** - Specify the password to change the Kerberos port. Default is 464.
[no] **health-check** *mon-name*	Check the server's health check status. Specify the name of an existing health check monitor (1- 63 characters).
[no] **health-check-disable**	Disable the configured health check configuration.
[no] **host** {*hostname* | *ipaddr*}	Hostname or IP address of the Windows server.
[no] **realm** *realm-name*	URL of the host realm for the authentication server.
[no] **support-apacheds-kdc**	Enable weak cipher (DES CRC/MD5/MD4) and merge AS-REQ in a single packet.
[no] **timeout** *value*	Specifies connection timeout to server, default is 10 seconds.

Default There are no default authentication-server profiles. When you create one, it has the default values specified in the table above.

Mode Configuration Mode

aam authentication service-group

Description Configure an authentication service group for multiple authentication servers. Can be used to create a group of multiple KDCs for a Kerberos relay.

Syntax

```
[no] aam authentication service-group service_group_name
{tcp | udp}
```

This command changes the CLI to the configuration level for the service-group, where the following commands are available.

Parameter	Description
[no] **health-check** *profile-name*	Enables a health check for the service group when user enters a configured health monitor.
[no] **health-check-disable**	Disables a health check configuration.
[no] **member** *profile-name*	Binds servers as members of the configured service-group.
[no] **method** *type*	Specifies load balancing method between servers in configured service-group. The default is **round-robin**.

Mode Configuration mode

aam authentication template

Description Configure an authentication template. You can use authentication templates to bind security resources to SLB resources (typically, an HTTP virtual port).

Syntax

```
[no] aam authentication template template-name
```

Parameter	Description
template-name	Name of the template (1-127 characters).

This command changes the CLI to the configuration level for the template, where the following commands are available.

Parameter	Description
[no] **account** *name*	Specify the name of an AD accoun t(1-63 characters).
[no] **accounting-server** *name*	Specify the name of a RADIUS accounting server.

Parameter	Description
[no] **accounting-service-group** *name*	Specify the name of an authentication service group for RADIUS accounting. This service group can only contain RADIUS servers.
[no] **auth-sess-mode** {cookie-based | ip-based}	Specify authentication session tracking mode for use of explicit proxy services. The available options are • **cookie-based** - Specify use of auth-key cookie to track if user has been authenticated. • **IP-based** - Specify use of client IP to determine if user has been authenticated.
[no] **cookie-domain** *domain*	Specify the domain scope for authentication (for example, **.exampledomain.com**).
[no] **cookie-domain-group** *id*	Specify the group ID (1-31 characters) to join in the specified **cookie-domain**.
[no] cookie-httponly-enable	Enable the cookie httponly attribute
[no] **cookie-max-age** *seconds*	Configure the maximum age for the authentication session cookie in seconds (0-2592000). The default is 604800 (1 week). When the cookie max-age is set to '0' the authentication session is valid till the browser is closed or the authentication session on ACOS is removed or timeout, the user must re-authenticate to access the ACOS again. If any other Cookie Max-Age value is set, the authentication key cookie will be saved by the browser and it will expire based on the set time.
[no] cookie-	Specify the value of SameSite attribute for

Parameter	Description
samesite strict/lax/none	AAM cookie **NOTE:** Set one of the option strict, lax, or none.
[**no**] **cookie-secure**-enable	Enable secure attribute for AAM cookies
[**no**] **forward-logout-disable**	Disable forward logout request to the back-end application server. The **logut-url** must first be configured before you can use this option.
[**no**] **log**	Enable or disable authentication logs for this template.
[**no**] **logon** *profile-name*	Name of a configured authentication logon profile.
[**no**] **logout-idle-timeout** *seconds*	Maximum amount of time an authenticated end-user session can be idle before being terminated by ACOS. You can specify 1-86400 seconds. The default is 300 seconds (5 minutes).
[**no**] **logout-url** *url-string* [...]	Web page to serve to end-users after they log out.
[**no**] **modify-content-security-policy**	Put redirect-uri or service-principal-name into CSP header to avoid CPS break authentication process.
[**no**] **redirect-hostname** *hostname*	Configure hostname for transparent-proxy authentication. The hostname can be 1-31 in length.
[**no**] **relay** *profile-name*	Name of a configured authentication-relay profile.
[**no**] **saml-idp** *idp-name*	Name of the SAML identity provider (1-63 characters).
[**no**] **saml-sp** *sp-name*	Name of the SAML service provider (1-63 characters)

Parameter	Description
[no] **server** *profile-name*	Name of a configured authentication-server profile. Use this option instead of the **service-group** option, if you have only one authentication server.
[no] **service-group** *group-name*	Name of a configured service group of authentication servers.
[no] **type** {**saml** | **standard**}	Specify the type of authentication template.
[no] captcha <captcha_profile>	Bind the captcha profile into the authentication template.
[no] logon <logon-name>	Name of the logon (1-127 characters).
[no] chain {server <server-name> | service-group <sg-name>} priority <1-5>	• `chain` - This option is mutual exclusively with `server` and `service-group`. • `server-name` - Name of the server. • `service-group` - Name of the service group. • `priority <1-5>` - Higher the number higher the priority and duplicate priority is not allowed. **NOTE:** Maximum five server or service-group in chain can be created.

Default There are no default authentication templates. When you create one, the defaults are described in the table above.

Mode Configuration Mode

aam authorization policy

Description Configure an authorization policy.

Syntax `[no] aam authorization policy policy-name`

This command changes the CLI to the configuration level for the policy, where the following commands are available.

Parameter	Description
[**no**] **attribute** *attr-num* {*attr-name* | **A10-AX-AUTH-URI**} **attr-type** *type* *operator* *attr-value*	Configure authorization attribute values. • *attr-num* – Attribute number, 1-32. • *attr-name* – Attribute name, either a custom name or A10-AX-AUTH-URI. • **attr-type** *type* – Data type of the attribute: ◦ **integer** ◦ **ip-addr** ◦ **string** • *operator* – Type of comparison to perform: ◦ **equal** ◦ **not-equal** ◦ **less-than** ◦ **more-than** ◦ **less-than-equal-to** ◦ **more-than-equal-to** ◦ **match** ◦ **sub-string** (The operators supported for a given data *type* differ depending on the type.) • *attr-value* – Value to be

Parameter	Description
	compared.
[**no**] **attribute-rule** *attr-num* {**and** | **or**} *attr-num*} ...	Rule for combining multiple attributes.
[**no**] **forward-policy-authorize-only**	Configure the policy to provide only server information for forward policy feature.
[**no**] **server** *profile-name*	Name of a configured authorization-server profile. Use this option instead of the **service-group** option, if you have only one authorization server.
[**no**] **service-group** *group-name*	Name of a configured service group of authorization servers.
[no] **attribute {1..32} <attr_ name> attr-type** number {equal | not-equal | less-than | more-than | less-than-equal-to | more-than-equal-to} <num>	Attribute type `number` which supports decimal representation. If the `CAPTCHA JSON` response has multiple levels. To check the attribute `action`, set the attribute name to `tokeninfo.action`.

Default Not set

Mode Configuration Mode

aam jwt-authorization

Description Configures the JWT authorization template which can bind to **AAM authorization policy**

Syntax

```
aam jwt-authorization <template-name>
```

Command	Description
[no] exp-claim-required	Specifies the exp claim, which is required for the JWT authorization.

Command	Description
[no] jwt-cache-enable	Enables caching of authorized JWT and skip verification and authorization for cached tokens.
[no] jwt-exp-default *seconds*	Specifies the default token expiration, if exp claim is not available (default 1800). You can configure the default JWT cache expiration time up to a maximum of 2592000 seconds.
[no] jwt-forwarding	Specifies that the JWT is not stripped, while forwarding the client request.
[no] log-level *level*	Specifies the JWT authorization syslog level (default value is **1**) • 0 = Log disable • 1 = Only log authorization fails (**default**) • 2 = Only log authorization success • 3 = Log all
[no] verification-cert *certificate-file*	Specifies the certificate to verify the JWT signature.
[no] verification-jwks *jwks-files*	Specifies the **jwks** file to verify the JWT signature.
[no] verification-secret *secret*	Specifies the secret to verify the JWT signature.

Default Not set

Mode Configuration mode

aam authentication oauth authorization-server

Description Configuring the OAuth authorization server

Syntax `aam authentication oauth authorization-server <NAME>`

Parameter	Description
[no] authorization-endpoint <NAME> <post | get>	Specify openid provider name for authorization.
[no] issuer <NAME>	Specify the URI for authorization which has two methods. Clients' browser sends data by POST (default) or GET.
[no] token-endpoint <NAME> <NAME> <post | get>	Specify URI for token exchange which also has POST (default) and GET two methods.
[no] verification-cert <NAME>	Specify certificate to verify ID token signature.
[no] verification-jwks <NAME>	Specify jwks file to verify ID token signature.

Default Not Set

Mode Configuration Mode

aam authentication oauth client

Description Configuring the authentication OAuth client.

Syntax `aam authentication oauth client <NAME>`

Parameter	Description
client-id <NAME>	Specify oauth client-id.
client-secret <NAME>	Specify oauth client secret for client.
grant-type <implicit | authorization-code | hybrid>	Specify oauth client grant type.

Parameter	Description
parameter-nonce-enable	Enable nonce parameter for authorization and token request.
redirection-endpoint <NAME>	Oauth client redirection endpoint service URL, this URL adds /js automatically when authorization-endpoint using GET method.
scope <NAME>	Specify request scope parameters (e.g. profile email address phone).
session-init-ttl <1-60>	TTL for Thunder to wait for first response from authorization server.
token-lifetime <1-2592000 | infinity>	Specify value of auth session expiring. If oauth servers don't response expired time, AX will use it. If we set to infinity, the auth session will never time out whatever value oauth servers' response.
type <openid-connect>	Allow to verify OpenID ID token.

Default Not Set

Mode Configuration Mode

aam authentication relay oauth

Description Configuring the authentication relay OAuth

Syntax

```
aam authentication relay oauth <NAME>
```

Parameter	Description
relay-type <access-token | id-token>	Specify token to relay in bearer schema.
relay-uri <all | equals | contains | starts-with | ends-with> <NAME>	Specify URI to trigger the oauth relay.

Default Access-token

Mode Configuration Mode

aam aaa-policy

Description Configure an AAA policy to bind configured templates, access-lists, and domains.

Syntax

```
[no] aam aaa-policy profile-name
```

Replace *profile-name* with the name of the AAA policy (1-63 characters).

After entering this command, enter the following command to designate rules for the AAA policy:

```
[no] aaa-rule rule-number
```

You can specify a rule index number 1-256.
This command drops you into AAA Rule configuration mode.

Default There are no default AAA policy profiles.

Mode Configuration Mode

Example Enter AAM AAA Rule configuration modaccounte:

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)#
```

access-list

Description Allows the user to specify which access list will be included in the AAA rule by using the following options

Syntax

```
access-list {1-199 | ip-name acl_name | ipv6-name acl_name}
```

Parameter	Description
1-199	ID of the access list.
ip-name *acl_name*	Specify the name of an IPv4 access list.
ipv6-name *acl_name*	Specify the name of an IPv6 access list.

Mode AAA Rule configuration mode

Example Include the IPv4 access list named **acl1** in the rule:

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)# access-list
ip-name acl1
```

NOTE: Standard access lists filter based on the source IP address, and you must specify a value between 1 and 99. Extended access lists filter based on the source and destination IP addresses, and you must specify a value between 100 and 199. You can also specify whether the access control list is an IPv4 or IPv6 filter.

action

Description Set the action that must be taken for this rule. It specifies whether the HTTP request is allowed (a match) or denied (no match).

Syntax

```
action {allow | deny}
```

Mode AAA Rule configuration mode

NOTE: The default value is **action** {**allow**}

Example Allow traffic that matches the rule.

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)# action allow
```

authentication-template

Description Specify the name of the authentication template you want to bind to this rule.

Syntax

```
[no] authentication-template template-name
```

Replace *template-name* with the name of an existing authentication template (1-127 characters).

Mode AAA Rule configuration mode

Example Bind the authentication template named **auth-tmplt-1** to this rule:

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)#
authentication-template auth-tmplt-1
```

authorize-policy

Description Specify the name of the authorization policy you want to bind to this rule.

Syntax

```
[no] authorize-policy policy-name
```

Replace *policy-name* with the name of an existing authorization policy (1-63 characters).

Mode AAA Rule configuration mode

Example Bind the authorization policy named **auth-policy-1** to this rule:

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)# authorize-
policy auth-policy-1
```

captcha-authz-policy

Description To bind the authorization policy for binding a captcha profile. An error message is displayed if the authorization policy does not bind a captcha profile

Syntax

```
captcha-authz-policy <authz_policy>
```

Default Not Set

Mode AAA Rule configuration mode

Example

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)#
authentication-template at
ACOS(config-aaa policy:policyname-aaa rule:...)# authorize-
policy ldap-authz
ACOS(config-aaa policy:policyname-aaa rule:...)# captcha-
authz-policy recaptchav3
```

domain-name

Description Specify the name of a specific domain you want to bind to this rule.

Syntax

```
[no] domain-name domain-name
```

Replace *domain-name* with the name of a domain (1-127 characters).

Mode AAA Rule configuration mode

NOTE: The domain rule will be used during authentication checking.

Example Bind the domain named **www.exampledomain.com** to this rule:

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)# domain-name
www.exampledomain.com
```

host

Description Specify a host to match for the AAA rule.

Syntax

```
[no] host {contains | ends-with | equals | starts-with}
hostname
```

Parameter	Description
contains	Match HOST if the request HTTP HOST header contains the specified *hostname*.
ends-with	Match HOST if the request HTTP HOST header ends with the specified *hostname*.

Parameter	Description
equals	Match HOST if the request HTTP HOST header is the same as the specified *hostname*.
starts-with	Match HOST if the request HTTP HOST header starts with the specified *hostname*.
hostname	Specify the host name (1-128 characters).

Mode AAA Rule configuration mode

Example Match the HOST if the HTTP HOST header contains “examplehost”:

```
ACOS(config)# aam aaa-policy matchhost
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)# host contains
examplehost
```

match-encoded-uri

Description Enable URL decoding for URI matching.

Syntax

```
[no] match-encoded-uri
```

Mode AAA Rule configuration mode

Example Configure the rule to enable URL decoding for URI matching:

```
ACOS(config)# aam aaa-policy policyname
ACOS(config-aaa policy:policyname)# aaa-rule 255
ACOS(config-aaa policy:policyname-aaa rule:...)# match-
encoded-uri
```

port

Description Specify a port to match for the AAA rule.

Syntax

```
[no] port portnum
```

Parameter	Description
portnum	Port number (1-65535).

Default If this option is not used and no port number is specified, the default is 0 (match all ports).

Mode AAA Rule configuration mode

uri

Description Specify the URI path for the AAA rule. This is useful in setting up varying authentication methods for different URLs.

Syntax

```
[no] uri {contains | ends-with | equals | starts-with} uri-string
```

Parameter	Description
contains	Match if the request URI contains the same string as the specified URI.
ends-with	Match if the request URI ends with the same string as the specified URI.
equals	Match if the entire request URI is the same as the specified URI.
starts-with	Match if the request URI starts with the same string as the specified URI.
uri-string	The URI string (1-128 characters).

Mode AAA Rule configuration mode

Usage This command configures URI checking, and you can specify what the path contains, can start with, can end with, and equals. The following text is an example of this command:

For more information about URIs, see RFC 2396.

Show Commands

clear aam authentication kcache

Description Clear Kerberos authentication cache.

Syntax

```
clear aam authentication session kcache [kerberos-relay-name]
```

Mode Privileged EXEC and all configuration levels.

clear aam authentication rdns

Description Clear Reverse DNS entries from ACOS AAM authentication cache table.

Syntax

```
clear aam authentication rdns {all | ipv4 ipv4_addr | ipv6
ipv6_addr}
```

Mode Privileged EXEC and all configuration levels.

clear aam authentication service-group

Description Clear authentication service-group statistics.

Syntax

```
clear aam authentication service-group {all | group-name}
```

Mode Privileged EXEC and all configuration levels.

clear aam authentication session

Description Clear authentication session table entries.

Syntax

```
clear aam authentication session all
```

or

Syntax

```
clear aam authentication session
source-addr {ipv4 ipv4-addr | ipv6 ipv6-addr}
[username username]
[vip virtual-server-name]
```

or

Syntax

```
clear aam authentication session username username
[source-addr {ipv4 ipv4-addr | ipv6 ipv6-addr}]
[vip virtual-server-name]
```

or

Syntax

```
clear aam authentication session vip virtual-server-name
[source-addr {ipv4 ipv4-addr | ipv6 ipv6-addr}]
[username username]
```

Parameter	Description
all	Clears all entries.
source-addr	Clears sessions with a specific IPv4 or IPv6 address.
username	Clears sessions with a specific username.
vip	Clears sessions with a specific virtual-server.

Mode Privileged EXEC and all configuration levels.

clear aam authentication statistics

Description Clear authentication statistics

Syntax

```
clear aam authentication statistics
[
aaa-policy |
aaa-rule |
logon spn-kerberos |
relay [type] |
saml-sp |
server [type]
]
[name]
```

Mode Privileged EXEC and all configuration levels.

clear aam authentication statistics jwt

Description Clear JWT authorization statistics

Syntax

```
clear aam authentication statistics jwt [name]
```

Default NA

Mode Privileged EXEC and all configuration levels.

clear aam authorization jwt cache

Description Clear cached JWTs

Syntax `clear aam authorization jwt cache [audience name]`

Default NA

Mode Privileged EXEC and all configuration levels

clear aam authentication saml idp status

Description Clear SAML Identity Provider status.

Syntax `clear aam authentication saml idp status`

Mode Privileged EXEC and all configuration levels.

show aam aaa-policy

Description Shows the AAA policy settings or RDNS records.

For the Multi-PU platforms, the aggregated RDNS records display from PU1 and PU2.

Syntax

```
show aam aaa-policy [rdns]
```

Parameter	Description
rdns	Show RDNS records.
name	Show AAA policy details, length: 1-63.

Mode Privileged EXEC and all configuration levels.

Example The following command shows the aggregated RDNS records from all PUs.

```
ACOS#show aam aaa-policy rdns
Type  Address                              DOMAIN
       TTL (Sec)
-------------------------------------------------------------------
-----------------
IPv4  1.1.1.1                              N/A
       1740
IPv4  1.1.1.2                              N/A
       1200
```

show aam authentication

Description Shows the authentication information.

Syntax

```
show aam authentication
```

show aam authentication account

Description Shows the authentication account settings.

Syntax

```
show aam authentication account [ kerberos-spn [account-name]
| password-retry [logon-name]
```

Parameter	Description
kerberos-spn	Shows Kerberos SPN account settings.
password-retry	Shows account password retry table. For the Multi-PU platforms, a new "PU" field displays to indicate the Processing Unit index (1 indicates PU1 and 2 indicates PU2).

Mode Privileged EXEC and all configuration levels.

Example The following command shows the account password retry summary from PU1 and PU2 and displays them separately. The PU field displays Processing Unit number in case of Multi-PU platform.

```
ACOS#show aam authentication account password-retry
Account password retry table
------------------------------------------------------------------
------------------
Account                                 user1
Logon Name                              basic
PU                                      1
Password failures                       2
TTL                                     1794
Locked Out                              Yes
------------------------------------------------------------------
------------------
Account                                 user1
Logon Name                              basic
PU                                      2
Password failures                       1
TTL                                     1796
Locked Out                              No
```

show aam authentication default-portal

Description Shows authentication default portal settings.

Syntax `show aam authentication default-portal`

Mode Privileged EXEC and all configuration levels.

show aam authentication jwks

Description Show JWKS file details

Syntax `show aam authentication jwks`

Default NA

Mode Privileged EXEC and all configuration levels

Example Show command output example:

```
ACOS# show aam authentication jwks
FILE NAME                                                                FILE SIZE
(byte)
--------------------------------------------------------------------------------
---------
jwk                                                                      649
jwk-periodic                                                             649
jwk-wrong-n                                                              633
jwk.bak                                                                  649
```

```
aXAPI

GET /axapi/v3/file/auth-jwks/oper
{
  "auth-jwks": {
    "oper" : {
      "file-list": [
        {
          "file":"jwk"
        },
```

```
        {
          "file":"jwk-periodic"
        },
        {
          "file":"jwk-wrong-n"
        },
        {
          "file":"jwk.bak"
        }
      ]
    },
    "a10-url":"/axapi/v3/file/auth-jwks/oper"
  }
}
```

Syntax `show aam authentication jwks`

Default NA

Mode Privileged EXEC and all configuration levels

show aam authentication klist

Description Shows a list of cached Kerberos tickets.

For the Multi-PU platforms, the Kerberos tickets under the principal name displays the aggregated principal name and PU1 and PU2 separately.

Syntax `show aam authentication klist [relay-profile-name]`

Replace *relay-profile-name* with the name of a configured authentication-relay profile.

Mode Privileged EXEC and all configuration levels.

Example The following command shows the Kerberos tickets from PU1 and PU2.

```
ACOS#show aam authentication klist
-----------------------
Ticket cache: MEMORY:kr1
```

```
Default principal: ax/cdpt@A10LAB.COM
PU 1:
Service principal: HTTP/sptest1.a10lab.com@A10LAB.COM
Client principal: dcadmin@A10LAB.COM
timespan: 03:35 29,Mar,2018 - 13:35 29,Mar,2018
renew untill: 03:35 05,Apr,2018
flags: FRA
Service principal: ax/cdpt@A10LAB.COM
Client principal: dcadmin@A10LAB.COM
timespan: 03:35 29,Mar,2018 - 13:35 29,Mar,2018
renew untill: 03:35 05,Apr,2018
flags: FRA
Service principal: krbtgt/A10LAB.COM@A10LAB.COM
Client principal: ax/cdpt@A10LAB.COM
timespan: 03:35 29,Mar,2018 - 13:35 29,Mar,2018
renew untill: 03:35 05,Apr,2018
flags: FRIA
PU2:
Service principal: HTTP/sptest1.a10lab.com@A10LAB.COM
Client principal: dcadmin@A10LAB.COM
timespan: 03:35 29,Mar,2018 - 13:35 29,Mar,2018
renew untill: 03:35 05,Apr,2018
flags: FRA
Service principal: ax/cdpt@A10LAB.COM
Client principal: dcadmin@A10LAB.COM
timespan: 03:35 29,Mar,2018 - 13:35 29,Mar,2018
renew untill: 03:35 05,Apr,2018
flags: FRA
Service principal: krbtgt/A10LAB.COM@A10LAB.COM
Client principal: ax/cdpt@A10LAB.COM
timespan: 03:35 29,Mar,2018 - 13:35 29,Mar,2018
renew untill: 03:35 05,Apr,2018
flags: FRIA
-----------------------
Ticket cache: MEMORY:kr2
Default principal: test@A10-TPLAB.COM
```

show aam authentication logon

Description Shows the configured AAM authentication-logon profiles.

Syntax

```
show aam authentication logon
{form-based profile-name | http-authenticate profile-name}
```

Mode Privileged EXEC and all configuration levels.

show aam authentication logon form-based

Description Shows details about authentication logon form-based

Syntax

```
show aam authentication logon form-based
```

Mode Privileged EXEC and all configuration levels.

Example The following example shows AAM Authentication logon form-based:

```
ACOS#show aam authentication logon form-based
Form-based Authentication Logon
Name                                    recaptcha
Type                                    form-based
Portal file                             sample-custom-portal-
recaptcha
Logon page name                         logon.html
Logon fail page name                    fail.html
Change password page name               cp.html
Challenge page name
New PIN page name
Next token page name
Action URL                              logon.fo
Change password page action URL
Change password notification page change URL
Change password notification page continue URL
Username variable name                  user
Password variable name                  pwd
Passcode variable name
CAPTCHA variable name                   g-recaptcha-response
Challenge variable name
New PIN variable name
```

```
Next token variable name
Change password username variable
Change password old password var
Change password new password var
Change password confirm password
Change password notification username variable
Change password notification old password var
Change password notification new password var
Change password notification confirm password
Login failure message
Authorization failure message
Retry count                                3
Account lock                               Disabled
Csp support none                           Enabled
HSTS timeout                               XXXsec
Disable change password link               No
```

show aam authentication logon http-authenticate

Description Shows details about authentication logon http-authenticate

Syntax

```
show aam authentication logon http-authenticate
```

Mode Privileged EXEC and all configuration levels.

Example The following example shows AAM Authentication logon form-based:

```
ACOS#show aam authentication logon http-authenticate
HTTP-Authenticate Authentication Logon
Name                                       basic
Type                                       http-authenticate
Mode                                       Basic
Basic-Realm
Retry count                                3
Account lock                               Disabled
Challenge response form
Challenge page name
Challenge variable name
New PIN page name
Next token page name
New PIN variable name
```

```
Next token variable name
HSTS timeout                                XXXsec
Disable change password link                No
```

show aam authentication portal

Description Shows the AAM logon portal archives that were imported to the ACOS device.

Syntax

```
show aam authentication portal [portal-archive-name]
```

Replace *portal-archive-name* with the filename of the imported archive for a logon portal.

Mode Privileged EXEC and all configuration levels.

show aam authentication portal-image

Description Shows authentication default portal images.

Syntax

```
show aam authentication portal-image
```

Mode Privileged EXEC and all configuration levels.

show aam authentication relay

Description Shows the configured AAM authentication-relay profiles.

Syntax

```
show aam authentication relay
{
form-based relay-name |
http-basic relay-name |
kerberos relay-name |
ws-federation relay-name
}
```

Replace *relay-name* with the name (1-63 characters) of the configured authentication relay.

Mode Privileged EXEC and all configuration levels

show aam authentication saml

Description Shows the configured SAML settings.

Syntax

```
show aam authentication saml
{idp | metadata | sp sp-name | sp-session sp-name}
```

Parameter	Descriptions
idp	Shows the SAML identity provider settings.
metadata	Shows the imported SAML metadata.
sp	Shows the SAML service provider settings.
sp-session	Shows the SAML service provider sessions. For the Multi-PU platforms, displays the aggregated SAML sp-session from PU1 and PU2.
sp-name	The name of the service provider.

Mode Privileged EXEC and all configuration levels.

Example The following command shows all SAML sp-session entries:

```
ACOS#show aam authentication saml sp-session
Service Provider: a10-azure-ad-test-saml-sp
NameID        Client addr       Id Provider      Auth Instant
   Expiration time
------------------------------------------------------------------
--------------------
kiSX9x0pYnTBd0jLXf2Z-rrU2OTg3mRz5jxqvcMM9Eg 172.29.50.76
https://sts.windows.net/b789a266-d9d4-4ac3-8f4b-aae1d15bc12a/
2023-05-15T03:26:26.696Z     2023-05-15 04:28:28
kiSX9x0pYnTBd0jLXf2Z-rrU2OTg3mRz5jxqvcMM9Eg 172.29.50.76
  https://sts.windows.net/b789a266-d9d4-4ac3-8f4b-
aae1d15bc12a/ 2023-05-15T03:15:30.491Z     2023-05-15 04:17:33
```

show aam authentication server

Description Shows the configured AAM authentication server profiles.

Syntax

```
show aam authentication server
{
bindings
  config [all-partitions | partition [shared | name]]
  [all-partitions | partition [shared | name]]
  [server-name] |
ldap [server-name] |
ocsp {server-name] |
radius {server-name] |
windows{server-name]
```

Parameter	Description
bindings	View server and service-group binding information. The **config** option also displays the server configuration. Specify a *server-name* to view the binding information for a single server only. You can also specify partition information to view server binding information by partition.
ldap	View profile for the specified LDAP authentication server.
ocsp	View profile for the specified OCSP authentication server.
radius	View profile for the specified Radius authentication server.
windows	View profile for the specified Windows authentication server.

Mode Privileged EXEC and all configuration levels.

show aam authentication service-group

Description Shows authentication service group settings.

For the Multi-PU platforms, the `service-group` displays aggregated health monitor output.

Syntax

```
show aam authentication service-group
{
```

```
all-partitions |
brief  [all-partitions | partition {shared | partition-name}]
|
config  [all-partitions | partition {shared | partition-name}]
|
sg-name
partition {shared | partition-name}
```

Parameter	Description
all-partitions	Shows authentication service group settings for all partitions.
partition *partition-name*	Shows authentication service group settings for the specified L3V partition only.
brief	Shows brief service group information.
config	Shows service group configuration information.
sg-name	Show the authentication details for the specified service group.

Mode Privileged EXEC and all configuration levels.

show aam authentication session

Description Shows general aFleX authentication session table statistics.

For the Multi-PU platforms, the authentication session ID for PU1 displays from 1 to 1048576, and for PU2 from 1048577 to 2097152.

Syntax

```
show aam authentication session
partition {all | shared | partition-name}
source-addr [specific-address] |
username [username] |
vip [virtual-server]]
```

Parameter	Description
partition	Shows sessions for the specified partition.

Parameter	Description
source-addr	Shows sessions with a specific address.
username	Shows sessions with a specific username.
vip	Shows sessions with a specific virtual-server.

NOTE: If your administrative session is in the shared partition, do not include the **partition** parameter.

Mode Privileged EXEC and all configuration levels.

Example Shows the authentication sessions from PU1 and PU2.

```
ACOS#show aam authentication session
TTL = Session Idle timeout (Sec), Lifetime = SAML
Token/Assertion Lifetime (Sec)
Total Sessions: 2
------------------------------------------------------------------
---------------------
ID      Type      VIP             User            Client IP
   Created Time
        VPort     Domain          Domain-group    TTL
   Lifetime
------------------------------------------------------------------
---------------------
1048578 STD       webvs           dcadmin
192.168.90.133  27-03-18 04:38:29
        23456                     0               297
   N/A
1       STD       webvs           user1
192.168.90.132  27-03-18 04:38:19
        23456                     0               287
   N/A
```

show aam authentication session-attributes

Description Shows the aFleX authentication session attributes.

Syntax

```
show aam authentication session-attributes
partition {all | shared | partition-name}
source-addr [specific-address] |
username [username] |
vip [virtual-server]]
```

Parameter	Description
partition	Show sessions for the specified partition.
source-addr	Shows sessions with a specific address.
username	Shows sessions with a specific username.
vip	Show sessions with a specific virtual-server.

NOTE: If your administrative session is in the shared partition, do not include the **partition** parameter.

Mode Privileged EXEC and all configuration levels.

show aam authentication session-with-attributes

Description Shows general aFleX authentication session information and aFlex session attributes.

Syntax

```
show aam authentication session-with-attributes
partition {all | shared | partition-name}
source-addr [specific-address] |
username [username] |
vip [virtual-server]]
```

Parameter	Description
partition	Show sessions for the specified partition.
source-addr	Shows sessions with a specific address.
username	Shows sessions with a specific username.
vip	Show sessions with a specific virtual-server.

NOTE: If your administrative session is in the shared partition, do not include the **partition** parameter.

Mode Privileged EXEC and all configuration levels.

show aam authentication statistics

Description Shows AAM statistics.

Syntax

```
show aam authentication statistics
aaa-policy [AAA-policy-name]|
aaa-rule [AAA-policy-name]|
form-based-relay [form-based relay-name]|
http-basic-relay [HTTP-basic relay-name]|
kerberos-relay [Kerberos-relay-name]|
ldap [LDAP-instance-name]|
ocsp [OCSP-server-name]|
ocsp-stapling[OCSP-server-name]|
radius [Radius-instance-name]|
saml-sp [SAML-service-provider-name]|
spn-kerberos [negotiate-logon-name]|
windows-kerberos[Windows-server-name]
```

Parameter	Description
aaa-policy	Shows authentication, authorization, and accounting (AAA) policy statistics.
aaa-rule	Shows AAA rule statistics.
form-based-relay	Shows authentication form-based relay statistics.
http-basic-relay	Shows authentication HTTP basic relay statistics.
kerberos-relay	Shows authentication Kerberos relay statistics.
ldap	Shows authentication LDAP statistics
negotiate-kerberos	Shows authentication Kerberos statistics of HTTP negotiate.
ocsp	Shows authentication OCSP server statistics.
ocsp-stapling	Shows authentication OCSP stapling statistics

Parameter	Description
`radius`	Shows authentication Radius statistics.
`saml-sp`	Shows SAML service provider statistics.
`windows-kerberos`	Shows authentication Windows Server Kerberos statistics.

Table 20 describes the fields in this command's output.

Table 20 : Description of the show aam authentication statistics Output

Column	Description
Engine Statistics	
Requests to Auth Daemon	Number of authentication requests that were handled by authentication daemon.
Responses from Auth Daemon	Number of authentication responses that were sent by authentication daemon to clients.
Requests to SAML	Number of SAML authentication requests that were handled by AAM.
Responses from SAML	Number of SAML authentication responses that were handled by AAM.
Misses	Number of authentication requests that failed because the end-users' credentials did not match the credentials in the ACOS AAM cache or on the back-end AAA server.
OCSP Stapling Requests to Auth Daemon	Number of OCSP authentication requests that were handled by authentication daemon..
OCSP Stapling Responses from Auth Daemon	Number of OCSP authentication responses that were sent by OCSP server to ACOS Device.
Engine aFleX Statistics	
Authorize success	Number of authorization requests that were handled by the ACOS authentication daemon.
Authorize failure	Number of authorization failure responses that

Table 20 : Description of the show aam authentication statistics Output

Column	Description
	were handled by the ACOS authentication daemon.
Auth Daemon Statistic	
Opened socket	Statistics used by ACOS network.
Open socket failed	
Get socket option failed	
Connect	Total number of attempts to set up a connection between AAM and a back-end AAA server.
Connect failed	Number of failed attempts to set up a connection between AAM and a back-end AAA server.
Created timer	Total number of times a cached set of user credentials, with an expiration timer, was successfully set up.
Create timer failed	Number of times an attempt to cache a set of user credentials failed.
DNS resolve failed	Number of failed attempts to resolve any DNS error.
Total request	Total number of AAA requests that were received from end-users and were handled by AAM.
Auth type	Lists request and response counters by each AAM-supported AAA type (for example, OCSP, RADIUS, LDAP, and Kerberos). • Request Normal– Number of requests that were forwarded by AAM to back-end AAA servers. • Request Dropped – Number of requests that were not forwarded by AAM to back-end AAA servers.

Table 20 : Description of the show aam authentication statistics Output

Column	Description
	• Response Success – Number of requests where the username and password that were entered by the user matched the credentials on the back-end AAA server and that resulted in successful authentications. • Response Failure – Number of requests that failed because the credentials that were entered by the user did not match the credentials on the back-end AAA server. • Response Error – Number of requests that failed because an error occurred in the exchange between AAM and the back-end AAA server. • Response Timeout – Number of requests sent by AAM to back-end AAA servers for which AAM did not receive a reply before the request timed out. • Response Other – Number of AAM errors not counted above.
Auth Daemon RADIUS Statistic	
Request	Number of accounting and authentication requests to AAM.
Authentication success	Number of successful RADIUS authentication requests that were handled by AAM. A request can succeed one of the following ways: • ACOS AAM cache has a current entry that matches the user's credentials. • Back-end RADIUS server had an entry that matches the user's credentials.
Authentication failure	Number of unsuccessful RADIUS authentication

Table 20 : Description of the show aam authentication statistics Output

Column	Description
	requests that were handled by AAM that failed because the credentials entered by the user were not found in the ACOS AAM cache or on the back-end server.
Authorize success	RADIUS Authorization requests successfully handled by AAM.
Authorize failure	RADIUS Authorization requests not successfully handled by AAM.
Access challenge	RADIUS CHAP challenge
Accounting-Request sent	Number of RADIUS accounting requests that were forwarded by AAM to a RADIUS server.
Accounting success	RADIUS Accounting requests successfully handled by AAM.
Accounting failure	RADIUS Accounting requests not successfully handled by AAM.
Timeout error	Number of RADIUS authentication and accounting requests that were forwarded by AAM to back-end RADIUS servers that timed out before AAM received a response from the server.
Job start error	
Polling control error	
Other error	Number of RADIUS AAM errors that were not included in the counters above.
Auth Daemon LDAP Statistic	
Request	Number of accounting and authentication requests to AAM.
Admin bind success	Number of times that AAM successfully logged in to a back-end LDAP server to verify administrator's credentials.

Table 20 : Description of the show aam authentication statistics Output

Column	Description
Admin bind failure	Number of times that AAM unsuccessfully attempted to login to a back-end LDAP server to verify administrator's credentials.
Bind success	Number of times that AAM successfully logged in to a back-end LDAP server to verify a user's credentials.
Bind failure	Number of times that AAM unsuccessfully attempted to login to a back-end LDAP server.
Search success	Number of times that the credentials that were entered by a user were found on the LDAP server.
Search failure	Number of times that the credentials that were entered by a user could not be found on the LDAP server.
Authorize success	Authorization statistics.
Authorize failure	
Timeout error	Number of LDAP authentication requests forwarded by AAM to a back-end server that timed out before AAM received a response from the server.
Job start error	
Polling control error	
TLS/SSL session created	Number of TLS/SSL sessions that were created.
TLS/SSL session failure	Number of TLS/SSL sessions that failed.
LDAPS idle connection number	Number of LDAPS idle connections in the pool.

Table 20 : Description of the show aam authentication statistics Output

Column	Description
LDAPS in-use connection number	Number of LDAPS in-use connections in the pool.
Other error	Number of LDAP AAM errors not included in the counters above.
Password expiry	Number of days the password is valid before expiration.
Password change success	Number of times the password change attempt by the user was successful.
Password change failure	Number of times the password change attempt by the user failed.
Auth Daemon Windows-Kerberos Statistic	
kerberos request send	Number of requests that were forwarded by ACOS to a back-end Kerberos Domain Controller (DC).
kerberos request get	Number of requests that were received from clients that AAM handled by using Kerberos.
Timeout error	Number of Kerberos authentication requests that were forwarded by AAM to a back-end server that timed out before AAM received a response from the server.
Job start error	
Polling error	
Other error	Number of Kerberos AAM errors not included in the counters above.
Password expiry	Number of days the password is valid before expiration.
Password change success	Number of times the password change attempt by the user was successful.
Password	Number of times the password change attempt

Table 20 : Description of the show aam authentication statistics Output

Column	Description
change failure	by the user failed.
Auth Daemon Kerberos-relay Statistic	
kerberos-relay request send	Number of kerberos requests from AAM.
kerberos-relay response get	Number of kerberos responses to AAM.
Timeout error	Number of Kerberos-relay authentication requests that were forwarded by AAM to a back-end server that timed out before AAM received a response from the server.
Job start error	
Polling error	
Other error	Number of Kerberos-relay AAM errors not included in the counters above.
Auth Daemon OCSP-Stapling Statistics	
Certificate Good	The specified certificate has been validated and can be used.
Certificate Revoked	The specified certificate has been revoked.
Certificate Unknown	The status of the specified certificate is unknown.
Kerberos SPN Statistic	
SPN kerberos requests	Number of SPN kerberos requests.
SPN kerberos response success	Number of successful SPN kerberos responses.
SPN kerberos response failure	Number of unsuccessful SPN kerberos responses.

Table 20 : Description of the show aam authentication statistics Output

Column	Description
SAML Statistic	
SP metadata export requests	Number of service provider metadata export requests.
SP metadata export successes	Number of successful service provider metadata export.
Login authn requests: 0	Number of login requests to the SAML service provider.
Login authn response	Number of login responses from the SAML service provider.
SLO requests	Number of requests to the SAML single logout service.
SLO successes	Number of successful single log outs.
SLO errors	Number of errors when handling single logout requests.
Other errors	Number of SAML errors not included in the counters above.
OAuth	
oauth	Count of authentication requested, failed, success, error, and other error.
oauth-relay	Count of reply request, success, and failure.

Mode Privileged EXEC and all configuration levels

Example The following example shows AAM statistics:

```
ACOS# show aam authentication statistics
Engine statistics:
-----------------------
Requests to Auth Daemon: 0
Responses from Auth Daemon: 0
Requests to SAML: 0
Responses from SAML: 0
Misses: 0
OCSP Stapling Requests to Auth Daemon: 0
```

```
OCSP Stapling Responses from Auth Daemon: 0
Engine aFleX statistics:
-----------------------
Authorize success: 0
Authorize failure: 0

Auth Daemon statistic:
-----------------------
Opened socket: 0
Open socket failed: 0
Get socket option failed: 0
Connect: 0
Connect failed: 0
Created timer: 0
Create timer failed: 0
DNS resolve failed: 0
Total request: 0
-------------------------------------------------------------
 \statistic Request Request Response Response Response
Response Response
Type\       Normal  Dropped Success  Failure  Error    Timeout
 Other
-------------------------------------------------------------
OCSP             0     0        0        0        0        0
    0
RADIUS           0     0        0        0        0        0
    0
LDAP             0     0        0        0        0        0
    0
Windows-KERBEROS 0     0        0        0        0        0
    0
KERBEROS-RELAY   0     0        0        0        0        0
    0
OCSP-STAPLING    0     0        0        0        0        0
    0
SPN-KERBEROS     0     0        0        0        0        0
    0
CAPTCHA          0     0        0        0        0        0
    0
-------------------------------------------------------------
```

```
Auth Daemon RADIUS statistic:
-----------------------
Request: 0
Authentication success: 0
Authentication failure: 0
Authorize success: 0
Authorize failure: 0
Access challenge: 0
Accounting-Request sent: 0
Accounting success: 0
Accounting failure: 0
Timeout error: 0
Job start error: 0
Polling control error: 0
Other error: 0

Auth Daemon LDAP statistic:
-----------------------
Request: 0
Admin bind success: 0
Admin bind failure: 0
Bind success: 0
Bind failure: 0
Search success: 0
Search failure: 0
Authorize success: 0
Authorize failure: 0
Timeout error: 0
Job start error: 0
Polling control error: 0
Other error: 0

Auth Daemon Windows-Kerberos statistic:
-----------------------
kerberos request send: 0
kerberos response get: 0
Timeout error: 0
Job start error: 0
Polling control error: 0
Other error: 0
```

```
Auth Daemon Kerberos-relay statistic:
-----------------------
kerberos-relay request send: 0
kerberos-relay response get: 0
Timeout error: 0
Job start error: 0
Polling control error: 0
Other error: 0

Auth Daemon OCSP-Stapling statistics:
-----------------------------------
Certificate Good: 0
Certificate Revoked: 0
Certificate Unknown: 0
OCSP failed: 0

Kerberos SPN statistic:
-----------------------
SPN kerberos request: 0
SPN kerberos response success: 0
SPN kerberos response failure: 0

SAML statistic:
-----------------------
SP metadata export requests: 0
SP metadata export successes: 0
Login authn requests: 0
Login authn responses: 0
SSO requests: 0
SSO successes: 0
SSO authorization failed: 0
SSO errors: 0
SLO requests: 0
SLO succeses: 0
SLO errors: 0
Other errors: 0

OAUTH statistic:
-----------------------
```

```
Auth requests: 0
Auth successes: 0
Auth failed: 0
Auth errors: 0
Relay requests: 0
Relay successes: 0
Relay failed: 0
Other errors: 0
Auth Daemon CAPTCHA statistic:
-----------------------
Request: 0
Verification success: 0
JSON response parse failure: 0
JSON response failure: 0
Attribute check failure: 0
Timeout error: 0
Other error: 0
Job start error: 0
Polling control error: 0
```

show aam authentication statistics captcha

Description shows the captcha authentication statistics.

Syntax

```
show aam authentication statistics captcha [<name>]
```

Mode Privileged EXEC and all configuration levels.

Example

```
Name  Request Verify-Succ Parse-Fail JSON-Fail Attr-Fail
Timeout Other
-------------------------------------------------------------------
--------
mtcaptcha  0    0           0          0         0         0
    0
v3         0    0           0          0         0         0
    0
```

show aam authentication statistics jwt

Description Show JWT authorization statistics

Syntax **show aam authentication statistics jwt** [*name*]

Default NA

Mode Privileged EXEC and all configuration levels

show aam authentication template

Description Shows the authentication template.

Syntax **show aam authentication template** [*template-name*]

Specify a *template-name* to view only the specified template.

Mode Privileged EXEC and all configuration levels.

show aam authorization jwt cache

Description Shows cached JWT summary.

For the Multi-PU platforms, a new “PU” field displays to indicate PU index (1 indicates PU1 and 2 indicates PU2).

Syntax **show aam authorization jwt cache** [**audience** *name*]

Default NA

Mode Privileged EXEC and all configuration levels.

Example Shows the jwt cached summary and from which PU the entry comes.

```
ACOS#show aam authorization jwt cache
Token cached: 0
Token cache hit: 0
Max token cache: 102400
-----------------------------------------------------------------
-----------------
```

```
ID      Issuer                                                  TTL
PU      Subject                 Audience                Client IP
------------------------------------------------------------------
------------------
1       http://vip1.a10-tplab.com                               86377
1       ytsai                   vip1
172.16.1.70
1       http://vip1.a10-tplab.com                               86397
2       ytsai                   vip1
172.16.1.70
```

show aam authorization policy

Description Shows details about your authorization policy.

Syntax

```
show aam authorization policy [policy-name]
```

Specify a specific *policy-name* to view detailed information for the specified policy.

Mode Privileged EXEC and all configuration levels.

Global Server Load Balancing

Global Server Load Balancing (GSLB) refers to load balancing applications on ACOS devices and global networks, to direct users to multiple data centers. Each data center consists of server farms that provide users with fast response time and redundancy to protect against the failure of a complete data center.

This reference lists the CLI configuration and show commands that apply specifically to GSLB.

Configuration Commands

delete geo-location

Description Delete or replace a custom geo-location database from the ACOS Device.

Syntax

```
delete geo-location {all | file-name}
```

Parameter	Description
all	Deletes all manually configured geo-locations from the configuration.
file-name	Delete the specified geo-location from the configuration.

Default N/A

Usage This command is available only if you have already imported a geo-location database file.

Mode Global configuration mode

gslb active-rdt

Description Configure global aRDT settings.

Syntax

```
[no] gslb active-rdt
{domain domain-name |
icmp interval seconds |port portnum |
retry num |
sleep seconds | timeout ms |
track seconds}
```

Parameter	Description
domain *domain-name*	Specifies the query domain. To measure the active-Round Delay Time (aRDT) for a client, the site ACOS Device sends queries for the domain name to a client's local DNS. An aRDT sample consists of the time between when the site ACOS Device sends a query and when it receives the response. Only one aRDT domain can be configured. It is recommended to use a domain name that is likely to be in the cache of each client's local DNS. The ACOS Device averages multiple aRDT samples together to calculate the aRDT measurement for a client. (See the description of **track** below.) The default domain is `google.com`.
icmp	Programs the device to use ICMP packets, instead of DNS requests, to calculate response delay time.
interval *seconds*	Specifies the number of seconds between queries. You can specify 1-16383 seconds. The default interval is 1 second.
port *portnum*	Specifies the port. You can specify ports 0-65535. The default port is 0.
retry *num*	Specifies the number of times GSLB will resend a query if there is no response. You can specify 0-16.

Parameter	Description
	The default is 3.
sleep *seconds*	Specifies the number of seconds GSLB stops tracking aRDT data for a client after a query fails. You can specify 1-300 seconds. The default is 3 seconds.
timeout *ms*	Specifies the number of milliseconds GSLB will wait for a reply before resending a query. You can specify 1-16383 ms. The default is 3000 ms.
track *seconds*	Specifies the number of seconds during which the ACOS Device collects samples for a client. The samples collected during the track time are averaged together, and the averaged value is used as the aRDT measurement for the client. You can specify 3-16383 seconds. The default is 60 seconds. The averaged aRDT measurement is used until it ages out. The aging time for averaged aRDT measurements is 10 minutes by default and is configurable on individual sites, using the **active-rdt aging-time** command in GSLB site configuration mode.

Default See descriptions.

Mode Global configuration mode

gslb dns action

Description Globally drop or reject DNS queries from the local DNS server.

Syntax

```
gslb dns action {drop | ignore | none | reject}
no gslb dns action
```

Parameter	Description
drop	Drops DNS queries that do not match any zone service.
ignore	Ignores DNS queries that do not match any zone service.
none	No action (default)
reject	Rejects DNS queries that do not match any zone service, and returns the “Refused” message in replies.

Default No action (`gslb dns action none`)

Mode Global configuration mode

gslb dns logging

Description Globally set DNS logging parameters. When this option is enabled, the GSLB DNS log messages appear in the ACOS log.

For more information, refer 'DNS Logging' in *Global Load Balancing Guide*.

Syntax

```
gslb dns logging {
 both [template  template-name] |
 query [template  template-name] |
 response [template  template-name] |
 none
}
no gslb dns logging
```

Parameter	Description
both [**template** *template-name*]	Log both the DNS query and response.
query [**template** *template-name*]	Log only the DNS query.
response [**template** *template-name*]	Log only the DNS response.
none	Do not log any DNS messages.

Default Disabled (`gslb dns logging none`)

Mode Global configuration mode

gslb geo-location

Description Configure a global geographic location by assigning a location name to a client IP address range. GSLB forwards client requests from addresses within the specified IP address range to the GSLB site that serves the location.

Syntax

```
[no] gslb geo-location location-name
```

Parameter	Description
location-name	Name of location. Use a period between string labels (ranges). Each range can contain up to 15 alphanumeric characters. Entire name can contain up to 127 characters. Example: `Asia.japan.123456789.xyz` ACOS Device can perform a partial match on geo-locations. Example: if IP 1.1.1.1 belongs to “Asia.japan”, but only “Asia” is configured, the ACOS Device still selects the proper site.

The command changes the CLI to the configuration level for the location, where the following location-related commands are available:

Command	Description
[no] ip *start-ip-addr* {**mask** *ip-mask* | *end-ip-addr*}	Beginning IPv4 address for the range. • **mask** *ip-mask* - Network mask • *end-ip-addr* - Ending IP address of the range

Command	Description
[**no**] **ipv6** *start-ipv6-addr* {**mask** *ipv6-mask* | *end-ipv6-addr*}	Beginning IPv6 address for the range. • **mask** *ipv6-mask* - Network mask • *end-ipv6-addr* - Ending IP address of range

Default N/A

Mode Global configuration mode

Usage Geographic location can be configured in a GSLB policy, which specifies using either the globally configured geographic location or the policy-configured location. (See geo-location and geo-location-match.)

Use manually configured geo-location mappings or load a mappings database, as described in gslb system geo-location load.

- If you manually map a geo-location to an GSLB site, GSLB uses the mapping.
- If no geo-location is configured for a GSLB site, GSLB automatically maps the service-ip to a geo-location in the loaded geo-location database.
- If a service-ip cannot be mapped to a geo-location, GSLB maps the site ACOS Device to a geo-location.

Example This example configures geographic location “US.CA.SanJose” for IP address range 100.1.1.1 through 100.1.1.125:

```
ACOS(config)# gslb geo-location US.CA.SanJose
ACOS(config-geo-location:US.CA.SanJose)# ip 100.1.1.1
100.1.1.125
ACOS(config-geo-location:US.CA.SanJose)#
```

gslb group

Description Configure GSLB group settings. GSLB controllers within a GSLB group automatically synchronize GSLB configuration information and data.

Syntax

```
[no] gslb group {default | group-name}
```

The command changes the CLI to the configuration level for the group, where the following group-related commands are available:

Other available commands are common to all CLI configuration levels. See the *CLI Reference*.

Command	Description
[no] auto-map [option]	Automatically creates IP-to-name mappings for resources within the zone. The *option* can be one of the following: • **data-interface** • **learn** • **mgmt-interface** • **primary** • **smart** This is disabled by default. This option is applicable only to GSLB zones that use wildcard service names
[no] config-anywhere	Allows GSLB to be configured on any group member, without restricting the changes to the master controller. This is disabled by default.
[no] config-merge	If this option is used and the current GSLB controller has the highest priority of all group members, then this current controller will attempt to retrieve the config file from the master GSLB controller before assuming control. This is disabled by default.
[no] config-save	Enables automatic configuration save on this GSLB group member when the configuration is saved on

Command	Description
	the group master. This is enabled by default.
[no] **dns-discover [resolve-to-ipv4 | resolve-to-ipv6 | resolve-to-ipv4-and-ipv6]**	Discover member via DNS protocol. When this option is used, you do not need to configure a primary IP address, because GSLB will send a DNS query (based on the group name) to discover other group members. For example, if group name is “group.example.com” then GSLB will send the DNS discover query with domain name “group.example.com”. • **resolve-to-ipv4**: Use A query only to resolve FQDN. This is the default query type. • **resolve-to-ipv6**: Use AAAA query only to resolve FQDN. • **resolve-to-ipv4-and-ipv6**: Use A as well as AAAA Query to resolve FQDN IPv4 or Ipv6 address.
[no] **enable**	Activates the ACOS Device’s membership in the GSLB controller group. This is disabled by default.
force-full-sync	Forces GSLB to synchronize full application configuration and GSLB related files from the master node to all the member nodes.
[no] **learn**	Enables the ACOS Device to learn the IP addresses of other group members from the group’s primary controllers. This is enabled by default.
[no] **primary**	Specifies the IP address of another group member, to be a primary member. After the GSLB process starts

Command	Description
ipaddr	on an ACOS Device, the device joins the controller group by connecting to the primary group members to exchange group management traffic. You can specify up to 15 primary members. Enter the command separately for each member. This is not set by default.
[**no**] **primary-ipv6** *ipv6_addr*	Specifies the IPv6 address (A:B:C:D:E:F:G:H) of another group member, to be a primary member. After the GSLB process starts on an ACOS Device, the device joins the controller group by connecting to the primary group members to exchange group management traffic. You can specify up to 15 primary members. Enter the command separately for each member. This is not set by default.
[**no**] **priority** *num*	Specifies the priority of the ACOS Device to become the master for the group. You can specify 1-255. The default is 100.
[**no**] **standalone**	Run GSLB Group in standalone mode. This is disabled by default.
[**no**] **suffix** *name*	This option allows you to configure the DNS suffix that will be used for dns-discovery. You can specify the suffix (or *name*) that GSLB will append to the domain name when sending the dns-discover query. For example, if the group name is “group” and the suffix is “example.com”, then the concatenated strings are sent in the DNS discovery query as “group.example.com”. This is not set by default.

Default See descriptions.

Mode GSLB Group Configuration Mode

Example

```
ACOS(config-group: default)# primary-ipv6 2001:201::3
```

gslb ip-list

Description Configure a list of IP addresses and group IDs to use as input to other GSLB commands.

Syntax

```
[no] gslb ip-list list-name
```

The command changes the CLI to the configuration level for the list, where the following IP-list-related commands are available:

(The other commands are common to all CLI configuration levels. See the *CLI Reference*.)

Parameter	Description
[no] ip *ipaddr* [*subnet-mask* | **/***mask-length*] **id** *group-id*	Creates an IP entry in the list. Based on the subnet mask or mask length, the entry can be a host address or a subnet address. The **id** option adds the entry to a group. The *group-id* can be 0-31.
[no] load *bwlist-name*	Loads the entries from a black/white list into the IP list.

Default None

Mode Global configuration mode

Usage You can configure an IP list in either of the following ways:

- Use a text editor on a PC or use the ACOS GUI to configure a black/white list, then load the entries from the black/white list into an IP list.
- Use this command to configure individual IP list entries.

Example The following commands configure a GSLB IP list and use the list to exclude IP addresses from aRDT data collection:

```
ACOS(config)# gslb ip-list iplist1
ACOS(config-gslb ip-list)# ip 192.168.1.0 /24 id 3
ACOS(config-gslb ip-list)# ip 10.10.10.10 /32 id 3
ACOS(config-gslb ip-list)# ip 10.10.10.20 /32 id 3
ACOS(config-gslb ip-list)# ip 10.10.10.30 /32 id 3
ACOS(config-gslb ip-list)# exit
ACOS(config)# gslb policy pol1
ACOS(config-gslb policy)# ip-list iplist1
ACOS(config-gslb policy)# active-rdt ignore-id 3
```

gslb policy

Description Configures a GSLB policy.

Syntax

```
[no] gslb policy {default | policy-name}
```

Parameter	Description
default	The default GSLB policy included in the software.
policy-name	Name of the policy, up to 63 alphanumeric characters.

This command changes the CLI to the configuration level for the specified GSLB policy.

Default N/A

Mode Global configuration mode

Example The following example creates a GSLB policy called “gslb-policy2”:

```
ACOS(config)# gslb policy gslb-policy2
ACOS(config-policy:gslb-policy2)#
```

Example The following example enables Certification Authority Authorization (CAA) in server mode:

```
ACOS(config)# gslb policy SODIUM
ACOS(config-policy:SODIUM)#dns server caa
```

active-rdt

Description Configure the active-Round Delay Time (aRDT) metric.

Syntax

```
[no] active-rdt
{
controller |
difference num |
enable |
fail-break |
ignore-id group-id |
keep-tracking |
limit ms |
prefer-dns-sticky difference num|
proto-rdt-enable |
samples num-samples |
single-shot |
skip count |
timeout seconds |
tolerance num-percentage
}
```

Parameter	Description
controller	This command enables GSLB Controller-based metrics on the device. GSLB Controller based metrics are not supported in IPv6 or L3V partition configurations. This is disabled by default.
difference *num*	Number from 0 to 16383 specifying the round-delay-time difference. The default is 0.
enable	Enable active-Round Delay Time for the given policy. This is disabled by default.
fail-break	Enables GSLB to stop if the configured aRDT limit in a policy is reached. The fail-break action depends on whether the GSLB controller is running in server mode or proxy mode: • Server mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns a blank

Parameter	Description
	response error to the client. • Proxy mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns the response from the back-end DNS server. Notes: • To configure the aRDT limit, use the **limit** option (describe below). • To configure GSLB to return a CNAME record as a backup, enable the backup-alias option using the **dns backup-alias** command at the configuration level for the policy. To configure the backup alias for a service within a zone, use the following command at the configuration level for the service: **dns-cname-record** *alias-name* **as-backup** This is disabled by default.
ignore-id *group-id*	Excludes the IP addresses in the specified IP list from aRDT data collection. Specify an ID from 0-31. (To configure an IP list, see gslb ip-list.) This is not set by default.
keep-tracking	Continues tracking of aRDT for clients after the track time expires. By default, GSLB stops collecting aRDT samples for a client (stops tracking the client) after the time has exceeded the number of seconds specified by the global aRDT track setting. This is disabled by default.
limit *ms*	Specifies the aRDT limit for the policy. This option is useful for applying site selection based on aRDT limits and geo-location. This option is required if you plan to use the DNS geoloc-policy option. You can

Parameter	Description
	specify 1-16383 ms. To configure aRDT limit by geo-location: 1. Enable the **`active-rdt bind-geoloc`** option on each GSLB site. 2. Enable the dns geoloc-policy option in the default GSLB policy, and enable the **`active-rdt`** option in the policies for geo-locations. If applicable, configure the aRDT limit. 3. On the service within the zone, enable the geo-location option and specify the GSLB policy to use for that location. The default limit is 16383 ms.
`prefer-dns-sticky` ***`difference`*** *num*	Integrates DNS sticky with aRDT and uses DNS sticky if available. Specify the mandatory difference value (in milliseconds) between 1-16383. The specified value is compared to the difference in response time between the current and previous best service IPs. The DNS sticky updates to the current best IP if the value exceeds the defined difference. Else, it remains unchanged.
`proto-rdt-enable`	his command configures GSLB controller-based metrics to includes both response times between 1) the controller and the originating LDNS server; and 2) the controller and the site device. When this option is disabled, the metric includes only the response time between the controller and the originating LDNS server. This is disabled by default.
`samples` *num-samples*	Number from 1 to 8 specifying the number of samples to collect.

Parameter	Description
	The default is 5.
single-shot	Collects a single sample only.
skip *count*	When single-shot is configured, this option determines the number of site ACOS Devices that can exceed their single-shot timeouts, without the aRDT metric itself being skipped by the GSLB ACOS Device during site selection. You can skip from 1-31 sites. This is disabled by default; multiple samples are taken at regular intervals. When enabled, the default skip is 3.
timeout *seconds*	When single-shot is configured, this option determines the number of seconds each site ACOS Device should wait for the DNS reply. If the reply does not arrive within the specified timeout, the site becomes ineligible for selection, in cases where selection is based on the aRDT metric. You can specify 1-255 seconds. The default timeout is 3 seconds.
tolerance *percentage*	Specifies how much the aRDT values must differ in order for GSLB to prefer one geo-location or site over another based on aRDT. The default is 10 percent.

Default Disabled. When you enable the aRDT metric, it has the default settings described in the table above.

Mode GSLB Policy

Usage aRDT measures the round-delay-time for a DNS query and reply between a site ACOS Device and the GSLB local DNS. This metric requires the GSLB protocol to be enabled both on the GSLB controller and on the site ACOS Devices.

Example The following example enable the aRDT metric, using default settings:

```
ACOS(config)# gslb policy gslbp2
```

```
ACOS(config-policy:gslbp2)# active-rdt enable
```

Example The following example enable the aRDT metric, using single-shot:

```
ACOS(config)# gslb policy gslbp3
ACOS(config-policy:gslbp3)# active-rdt enable
ACOS(config-policy:gslbp3)# active-rdt single-shot
ACOS(config-policy:gslbp3)# active-rdt skip 3
```

Example The following example enable the aRDT metric, using single-shot:

```
ACOS(config)# gslb policy gslbp4
ACOS(config-policy:gslbp4)# active-rdt enable
ACOS(config-policy:gslbp4)# dns sticky /24
ACOS(config-policy:gslbp4)# active-rdt prefer-dns-sticky
difference 15
```

active-servers

Description Configure the Active-Servers metric, which prefers the VIP with the highest number of active servers.

Active-servers is a measure of the number of active real servers bound to a virtual port residing on a GSLB site.

Syntax

```
[no] active-servers fail-break
```

Parameter	Description
fail-break	Enables GSLB to stop if the number of active servers for all services is 0. The fail-break action depends on whether the GSLB controller is running in proxy mode or server mode: • Server mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns a SERVFAIL error to the client. • Proxy mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns the response from the back-end DNS server.

NOTE: Use the active-servers-enable command to enable or disable selecting the service-IP with the highest number of active servers.

Default Disabled

Mode GSLB Policy

Usage Use this command to eliminate inactive real servers from being eligible for selection.

Example The following example enables the Active-Servers metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# active-servers-enable
ACOS(config-policy:pol1)# active-servers fail-break
ACOS(config-policy:pol1)#
```

active-servers-enable

Description Enable or disable selecting the service-IP with the highest number of active servers:

Syntax

```
[no] active-servers-enable
```

Default Disabled by default

Mode GSLB Policy

Example The following example enables the Active-Servers metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# active-servers-enable
ACOS(config-policy:pol1)# active-servers fail-break
```

admin-ip

Description Allows you to assign administrative weights to IP addresses.

Syntax

```
[no] admin-ip top-only
```

The **top-only** parameter selects only the top prioritized record.

NOTE: To configure GSLB to return only the top prioritized IP address in query responses, also enable the **dns selected-only** option. Use admin-ip-enable command to enable or disable admin IP prioritization.

Default Disabled

Mode GSLB Policy

Usage The prioritized list is sent to the next metric for further evaluation. If **admin-ip** is the last metric, the prioritized list is sent to the client. To configure the list of admin-preferred addresses for a service, use the **admin-ip** command at the service configuration level for the gslb zone.

admin-ip-enable

Description Enable or disable admin IP prioritization.

Syntax

```
[no] admin-ip-enable
```

Default Disabled.

Mode GSLB Policy

admin-preference

Description Enable or disable the Admin-Preference metric, which prefers the site whose SLB device has the highest administratively set weight.

Syntax

```
[no] admin-preference
```

Default Disabled

Mode GSLB Policy

Usage To set the GSLB Admin-Preference value for a site, use the **admin-preference** command at the configuration level for the SLB device within the gslb site.

Example The following command enables the Admin-Preference metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# admin-preference
```

alias-admin-preference

Description Enable or disable the Alias Admin Preference metric, which selects the DNS CNAME record with the highest administratively set preference. This metric is similar to the Admin Preference metric, but applies only to DNS CNAME records.

Syntax

```
[no] alias-admin-preference
```

Default Disabled

Mode GSLB Policy

Usage Metric order does not apply to this metric. When enabled, this metric always has high priority.

To configure the Alias Admin Preference metric:

1. At the configuration level for the gslb service-ip, use the **admin-preference** *preference* command to assign an administrative preference to the DNS CNAME record for the service.
2. At the configuration level for the GSLB policy:
   - Use the **alias-admin-preference** command to enable the Alias Admin Preference metric.
   - Enable one or both of the following DNS options, as applicable to your deployment.
   - DNS backup-alias
   - DNS geoloc-alias
3. If using the **backup-alias** option, use the **dns-cname-record as-backup** option on the service.

auto-map

Description Enable auto-mapping of the specified resource type within the policy.

Syntax

```
[no] auto-map [module-disable resource-type | ttl num]
```

Parameter	Description
module-disable	Specify what resource-types you want to disable auto-mapping for.

Parameter	Description
resource-type	By default, all modules have Auto Map M.
ttl *num*	Specify a Time-to-Live for auto-mapping. The default is 300 seconds. You can specify from 1-65535 seconds. The default TTL is 300 seconds.

Default See descriptions.

Mode GSLB Policy

Related Commands:

- gslb system auto-map module
- gslb system auto-map ttl

bw-cost

Description Configure the BW-Cost metric. This mechanism queries the bandwidth utilization of each site, and selects the site(s) whose bandwidth utilization has not exceeded a configured threshold during the most recent query interval.

```
[no] bw-cost fail-break
```

The bandwidth cost fail-break enables GSLB to stop if the current BW-Cost value is over the limit. The fail-break action depends on whether the GSLB controller is running in proxy mode or server mode:

- Server mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns a SERVFAIL error to the client.
- Proxy mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns the response from the back-end DNS server.

NOTE: Use the bw-cost-enable command to enable selection of the site with the smallest bandwidth cost.

Default Disabled

Mode GSLB Policy

Example The following command enables the BW-Cost metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# bw-cost-enable
ACOS(config-policy:pol1)# bw-cost fail-break
```

bw-cost-enable

Description Enable selection of the site with the smallest bandwidth cost.

Syntax

```
[no] bw-cost-enable
```

Default Disabled.

Mode GSLB Policy

Example The following command enables the BW-Cost metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# bw-cost-enable
ACOS(config-policy:pol1)# bw-cost fail-break
ACOS(config-policy:pol1)#
```

capacity

Description Configure the TCP/UDP Session-Capacity metric. This mechanism provides a way to shift load away from a site before the site becomes congested.

Syntax

```
[no] capacity {enable | fail-break | threshold percentage}
```

Parameter	Description
enable	Enables selection of the service-IP with the highest available connection capacity.
fail-break	Enables GSLB to stop if the session utilization on all site SLB devices is over the threshold. The fail-break action depends on whether the GSLB controller is running in proxy mode or server mode:

Parameter	Description
	• Server mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns a SERVFAIL error to the client. • Proxy mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns the response from the back-end DNS server.
threshold *percentage*	Number from 0 to 100 specifying the maximum percentage of a site ACOS Device session table that can be used. If the session table utilization is greater than the specified percentage, the GSLB controller prefers other sites over this site. The default threshold is 90 percent.

Default Disabled. See descriptions for default values when the capacity metric is enabled.

Mode GSLB Policy

Usage Let us consider that Site A's maximum session capacity is 800,000 and Site B's maximum session capacity is 500,000. If the Session-Capacity threshold is set to 90, then for Site A the capacity threshold is 90% of 800,000, which is 720,000. Likewise, the capacity threshold for Site B is 90% of 500,000, which is 450,000.

This metric requires the GSLB protocol to be enabled both on the GSLB controller and on the site ACOS Devices.

Example The following command enables the capacity metric at the default value of 90% utilization of TCP/UDP session capacity:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# capacity enable
```

connection-count-by-site

Description Configure the connection-count-by-site metric.

Syntax

```
[no] connection-count-by-site
 enable
```

Parameter	Description
enable	Enables the connection-count-by-site metric.

Default Disabled.

Mode GSLB Policy

Usage This command is only applicable to virtual IPs that are bound under SLB devices within a GSLB site. The metric is used in case of scaleout service IPs that provide support for multiple devices in a scaleout cluster setup. The metric considers the connection count of virtual IP servers in a site. Based on the aggregated count, ACOS redirects the traffic to the site with the lower count.

For details on configuration, see 'Connection Count by Site' section in the *Global Server Load Balancing Guide*.

NOTE: The current connection metrics is not calculated for service IP records used as IP servers directly under a site.

Example The following command sets the connection-count-by-site metric for the **test_policy**.

```
ACOS(config)# gslb policy test_policy
ACOS(config-policy:test_policy)#connection-count-by-site
enable
```

connection-load

Description Configure the Connection-Load metric, which prefers sites that have not exceeded their thresholds for new connections.

Syntax

```
[no] connection-load
{
enable |
fail-break |
limit number-of-connections |
samples number-of-samples interval seconds
}
```

Parameter	Description
enable	Enables the Connection-Load metric.
fail-break	Enables GSLB to stop if the connection load for all sites is over the limit. Fail-break action depends on whether the GSLB controller runs in proxy mode or server mode: • Server mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns a SERVFAIL error. • Proxy mode: If a backup-alias is configured, the GSLB controller returns the backup-alias to the client; otherwise, the controller returns the response from the back-end DNS server.
limit *number-of-connections*	Number that specifies the maximum average number of new connections per second the site ACOS Device can have. You can specify from 1 to 999999999 (999,999,999). The default limit is not set (unlimited).
samples *number-of-samples* **interval** *seconds*	Number of samples for the SLB device (the site ACOS Device) to collect, and the number of seconds between each sample. You can specify 1-8 samples and an interval of 1-60 seconds. The default number of samples is 5, and the default interval is 5 seconds.

Default Disabled. See descriptions for default values when the Connection-Load metric is enabled.

Mode GSLB Policy

Usage This command applies only to GSLB selection of a site. The command does not affect the number of connections the site ACOS Device itself allows.

This metric requires the GSLB protocol to be enabled both on the GSLB controller and on the site ACOS Devices.

Example The following command sets the connection load limit to 1000 new connections:

```
ACOS(config-policy:pol1)# gslb policy pol1
ACOS(config-policy:pol1)# connection-load limit 1000
```

dns action

Description The **dns action** command enables GSLB to perform the DNS actions specified in the service configurations.

To configure the DNS action for a service, use the **action** *action-type* command at the configuration level for the gslb zone.

The **no dns action** command restores the default value

Syntax

```
[no] dns action
```

Default Disabled

Mode GSLB Policy Configuration Mode

Example This command enables GSLB to perform the DNS actions specified in service configurations.

```
ACOS(config)# gslb policy oxygen
ACOS(config-policy:oxygen)# dns action
```

dns active-only

Description The **dns active-only** command removes IP addresses from DNS replies when those addresses fail health checks. If none of the IP addresses in the DNS reply pass the health check, the ACOS Device does not use this metric, because it results in an empty address list.

The **fail-safe** option returns a list of server IP addresses for failed servers to the client. Without this option, IP addresses of failed servers are omitted from the reply.

The **no dns active-only** command restores the default mode of disabling the removal of IP addresses that fail health checks from DNS replies.

Syntax

```
dns active-only [MODE]
[no] dns active-only [MODE]
```

Parameter	Description
MODE	Specifies the information returned to the client. Valid options include: • <no parameter> omits IP addresses of failed servers from reply • **fail-safe** includes IP addresses of failed servers in client reply.

Default Disabled.

Mode GSLB Policy Configuration Mode

Example This command programs the ACOS Device to remove IP address from DNS of device that fail health check. The address of failed devices are not returned to the client.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns active-only
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns active-only
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to remove IP address from DNS of device that fail health check and returns the address list of failed devices to the client.

```
ACOS(config-policy:OXYGEN)# dns active-only fail-safe
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns active-only fail-safe
ACOS(config-policy:OXYGEN)#
```

Example This command sets the ACOS Device to ignore health check failure in its DNS replies.

```
ACOS(config-policy:OXYGEN)# no dns active-only fail-safe
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns addition-mx

Description The **dns addition-mx** command programs the ACOS Device to append MX records in the *additional section* of replies for A records when the device is configured for DNS proxy or cache mode.

Syntax

```
[no] dns addition-mx
```

Default Disabled

Mode GSLB Policy Configuration Mode

Example This command programs the ACOS Device to append MX records to the additional section of replies for A records.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns addition-mx
```

dns auto-map

Description The **dns auto-map** command enables the automatic creation of A and AAAA records for IP resources configured on the ACOS Device.

The **no dns auto-map** command disables automatic creation of A and AAAA records.

Syntax

```
[no] dns auto-map
```

Default Disabled

Mode GSLB Policy Configuration Mode

Example The following command enables the automatic creation of A and AAAA records for IP resources configured on the ACOS Device.

```
ACOS(config)# gslb policy OXYGEN
```

```
ACOS(config-policy:OXYGEN)# dns auto-map
```

dns backup-alias

Description The **dns backup-alias** command returns the alias CNAME record configured for the service, if GSLB does not receive an answer to a query for the service and no active DNS server exists. This option is valid in server mode or proxy mode.

To configure the backup alias for a service within a zone, use the **dns-cname-record** command at the configuration level for the service.

The **no dns backup-alias** command restores the default of not returning the alias CNAME record.

Syntax

```
dns backup-alias
[no] dns backup-alias
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Example This command configures the ACOS Device to return the alias CNAME record configured for the service when GSLB does not receive an answer to a query for the service when no active DNS server exists.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns backup-alias
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns backup-alias
ACOS(config-policy:OXYGEN)#
```

Example This command configures the ACOS Device to not return the alias CNAME record configured for the service when GSLB does not receive an answer to a query for the service when no active DNS server exists.

```
ACOS(config-policy:OXYGEN)# no dns backup-alias
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns backup-server

Description The **dns backup-server** command designates one or more backup servers that can be returned to the client if the primaries should fail.

The **no dns backup-server** command removes the designation.

Syntax

```
dns backup-server
no dns backup-server
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Example This command designates the ACOS Device as a backup server that can be returned to the client if the primaries should fail.:

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns backup-server
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns backup-server
ACOS(config-policy:OXYGEN)#
```

Example This command removes the backup server designation.

```
ACOS(config-policy:OXYGEN)# no dns backup-server
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns cache

Description The **dns cache** command enables the GSLB ACOS Device to cache DNS replies. The ACOS Device uses information in the cached DNS entries to reply to subsequent client requests, as opposed to sending a new DNS request for every client query.

When this option is enabled, the ACOS Device caches a DNS reply for the duration of the TTL in the reply when the aging time parameter is set to zero. To override the entry TTL, set the cache aging time to a value greater than zero.

The **no dns cache** command disables the GSLB ACOS Device from caching DNS replies.

Syntax

```
dns cache [DURATION]
no dns cache
```

Parameter	Description
DURATION	Specifies site location mode. Valid options include • <no parameter> cache period is specified in DNS reply • **aging-time 0** cache period is specified in DNS reply • **aging-time** *period* cache period (seconds) Value ranges from 1 to 1000000000 (one billion)

Default Disabled.

Mode GSLB Policy Configuration Mode

Example The following command enables the caching of DNS replies and set the TTL to the period specified in the reply.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns cache
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns cache
ACOS(config-policy:OXYGEN)#
```

Example This command sets the TTL to 30 minutes.

```
ACOS(config-policy:OXYGEN)# dns cache aging-time 1800
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns cache aging-time 1800
ACOS(config-policy:OXYGEN)#
```

Example This command resets the TTL to the period set to the period specified in the reply.

```
ACOS(config-policy:OXYGEN)# dns cache aging-time 0
```

```
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns cache
ACOS(config-policy:OXYGEN)#
```

Example The command disables the GSLB ACOS Device from caching DNS replies.

```
ACOS(config-policy:OXYGEN)# no dns cache
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns cname-detect

Description The **dns cname-detect** command enables CNAME response mode. When the ACOS Device is in CNAME response mode, it applies the zone and service policy to the CNAME record instead of applying it to the address record. When CNAME response mode is disabled, the zone and service policy is applied to the address record. Executing this command restores the CNAME response mode setting of enabled.

The **no dns cname-detect** command disables CNAME response mode on the ACOS Device.

Syntax

```
dns cname-detect
no dns cname-detect
```

Default Enabled

Mode GSLB Policy Configuration Mode

Example This command disables CNAME response mode.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# no dns cname-detect
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  no dns cname-detect
ACOS(config-policy:OXYGEN)#
```

Example This command enables CNAME response mode.

```
ACOS(config-policy:OXYGEN)# dns cname-detect
ACOS(config-policy:OXYGEN)# show run | sec gslb
```

```
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns delegation

Description The **dns delegation** command enables sub-zone delegation mode. When in sub-zone delegation mode, the device delegates authority or responsibility for a portion of the DNS name space from the parent domain to a separate sub-domain which may reside on one or more remote servers and may be managed by someone other than the network administrator who is responsible for the parent zone.

The **no dns delegation** command disables sub-zone delegation mode.

Syntax

```
dns delegation
no dns delegation
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands enable sub-zone delegation mode.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns delegation
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns delegation
ACOS(config-policy:OXYGEN)#
```

Example These command disables sub-zone delegation mode.

```
ACOS(config-policy:OXYGEN)# no dns delegation
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns external-ip

Description The **dns external-ip** command returns the external IP address configured for a service IP. If this option is disabled, the internal address is returned instead..

The external IP address must be configured on the service IP. Use the **external-ip** command at the configuration level for the service IP.

The **no dns external-ip** command disables the option of returning the external IP address configured for a service IP.

Syntax

```
dns external-ip
no dns external-ip
```

Default Enabled.

Mode GSLB Policy Configuration Mode

Example These commands disable the option of returning the external IP address configured for a service IP address.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# no dns external-ip
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  no dns external-ip
ACOS(config-policy:OXYGEN)#
```

Example These commands enable the option of returning the external IP address configured for a service IP address.

```
ACOS(config-policy:OXYGEN)# dns external-ip
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns external-soa

Description The **dns external-soa** command programs the ACOS Device to replace the internal SOA record with an external SOA record, preventing external clients from gaining accessing internal information.

The external SOA record must be configured in the GSLB zone. (Use the **external-soa record** command at the GSLB zone configuration level.)

The **no dns external-soa** command disables this option. When this option is disabled, the internal address is returned.

Syntax

```
dns external-soa
no dns external-soa
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands programs the ACOS Device to replace the internal SOA record with an external SOA record.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns external-soa
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns external-soa
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to return the internal address..

```
ACOS(config-policy:OXYGEN)# no dns external-soa
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns geoloc-action

Description The **dns geoloc-action** command programs the ACOS Device to perform the DNS traffic handling action specified for the client's geo-location. The action is specified as part of service configuration in a zone.

To configure the DNS action for a service, use the **geo-location** *location-name action-type* command at the configuration level for the service.

The **no dns geoloc-action** command restores the default value, where the ACOS Device does not performing the DNS traffic handling action.

Syntax

```
dns geoloc-action
no dns geoloc-action
```

Default Default.

Mode GSLB Policy Configuration Mode

Example These commands programs the ACOS Device to perform the DNS traffic handling action specified for the client's geo-location.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns geoloc-action
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns geoloc-action
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to not perform the DNS traffic handling action specified for the client's geo-location.

```
ACOS(config-policy:OXYGEN)# no dns geoloc-action
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns geoloc-alias

Description The **dns geoloc-alias** command configures the ACOS Device to return the alias name configured for the client's geo-location.

The **no dns geoloc-alias** command configures the ACOS Device to not return alias name configured for the client's geo-location.

Syntax

```
dns geoloc-alias
no dns geoloc-alias
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands configure the ACOS Device to return the alias name configured for the client's geo-location.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns geoloc-alias
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns geoloc-alias
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to not return alias name configured for the client's geo-location.

```
ACOS(config-policy:OXYGEN)# no dns geoloc-alias
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns geoloc-policy

Description The **dns geoloc-policy** command configures the ACOS Device to use the GSLB policy assigned to the client's geo-location.

The **no dns geoloc-policy** command configures the ACOS Device to not use the GSLB policy assigned to the client's geo-location.

Syntax

```
dns geoloc-policy
no dns geoloc-policy
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Description These commands configure the ACOS Device to use the GSLB policy assigned to the client's geo-location.

Example The **no dns geoloc-policy** command configures the ACOS Device to not use the GSLB policy assigned to the client's geo-location.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns geoloc-policy
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns geoloc-policy
ACOS(config-policy:OXYGEN)#
```

Example This command configures the ACOS Device to not use the GSLB policy assigned to the client's geo-location.

```
ACOS(config-policy:OXYGEN)# no dns geoloc-policy
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns hint

Description The **dns hint** command manages the appearance of hints that appear in the Additional Section of DNS responses. Hints are A or AAAA records that are sent in the response to a client's DNS request. These records provide a mapping between the host names and IP addresses.

The **hint** option applies to the following record types: NS, MX, and SRV.

The **no dns action** command restores the default value of appending hints in the Additional section, which is equivalent to the addition option.

Syntax

```
dns hint LOCATION
no dns hint
```

Parameter	Description
LOCATION	Specifies the section where hints are appended. Options include: • **addition** Appends hints in the Additional Section (default). • **answer** Appends hints in the Answer Section. • **none** Does not append hints in the DNS response.

Default Hints are enabled and appended in the Additional section..

Mode GSLB Policy Configuration Mode

Example These commands configure the ACOS Device to append hints in the Answer section of the DNS response.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns hint answer
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns hint answer
ACOS(config-policy:OXYGEN)#
```

Example This command configure the ACOS Device to not append hints to the DNS response.

```
ACOS(config-policy:OXYGEN)# dns hint none
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns hint none
ACOS(config-policy:OXYGEN)#
```

Example This command configures the ACOS Device to append hints in the Answer section of the DNS response.

```
ACOS(config-policy:OXYGEN)# dns hint addition
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns ip-replace

Description The **dns ip-replace** command configures the ACOS Device to replace the IP addresses in DNS replies with the service IP addresses configured for the service.

To configure the service IP addresses, use the **service-ip** command at the configuration level for the service.

The **no dns ip-replace** command restores the ACOS default behavior of not replacing the IP addresses in DNS replies with the service IP addresses configured for the service.

Syntax

```
dns ip-replace
no dns ip-replace
```

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands configure the ACOS Device to replace the IP addresses in DNS replies with the service IP addresses configured for the service.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns ip-replace
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
```

```
  dns ip-replace
ACOS(config-policy:OXYGEN)#
```

Example This command restores the ACOS default behavior of not replacing the IP addresses in DNS replies with the service IP addresses configured for the service.

```
ACOS(config-policy:OXYGEN)# no dns ip-replace
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns ipv6 mapping

Description The **dns ipv6 mapping** command specifies the ACOS Device response to IPv6 DNS query. You can enable one of these options.

- **addition** – Append AAAA records in the DNS Addition section of replies.
- **answer** – Append AAAA records in the DNS Answer section of replies.
- **exclusive** – Replace A records (IPv4 address records) with AAAA records.
- **replace** – Reply with AAAA records only.

The **dns ipv6 mapping** command restores the default behavior of not using AAAA records to respond to IPv6DNS queries.

Syntax

```
dns ipv6 mapping ACTION
no dns ipv6 mapping
```

Parameter	Description
ACTION	Specifies response actions to IPv6 DNS queries. Valid options include: • **addition** – Append AAAA records in DNS Addition section of replies. • **answer** – Append AAAA records in the DNS Answer section of replies.

Parameter	Description
	• **exclusive** – Replace A records (IPv4 address) with AAAA records. • **replace** – Reply with AAAA records only.

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands program the ACOS Device to append AAAA records in the DNS Addition section of replies to IPv6 DNS queries.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns ipv6 mapping addition
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns ipv6 mapping addition
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to append AAAA records in the DNS Answer section of replies to IPv6 DNS queries.

```
ACOS(config-policy:OXYGEN)# dns ipv6 mapping answer
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns ipv6 mapping answer
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to replace A record with AAAA records in response to IPv6 DNS queries.

```
ACOS(config-policy:OXYGEN)# dns ipv6 mapping exclusive
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns ipv6 mapping exclusive
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to use AAAA records only in response to IPv6 DNS queries.

```
ACOS(config-policy:OXYGEN)# dns ipv6 mapping replace
ACOS(config-policy:OXYGEN)# show run | sec gslb
```

```
gslb policy OXYGEN
  dns ipv6 mapping replace
ACOS(config-policy:OXYGEN)#
```

Example This command programs the ACOS Device to not use AAAA records respond to IPv6 DNS queries.

```
ACOS(config-policy:OXYGEN)# no dns ipv6 mapping
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns ipv6 mix

Description The **dns ipv6 mix** command configures the ACOS Device to return AAAA and A records in the same response.

The **no dns ipv6 mix** command disables the ability to return AAAA and A records in the same response.

Syntax

```
dns ipv6 mix
no dns ipv6 mix
```

Default Disabled

Mode GSLB Policy Configuration Mode

Example These commands configure the ACOS Device to return AAAA and A records in the same response.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns ipv6 mix
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns ipv6 mix
ACOS(config-policy:OXYGEN)#
```

Example This command disables the ability to return AAAA and A records in the same response.

```
ACOS(config-policy:OXYGEN)# no dns ipv6 mix
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns ipv6 smart

Description The **dns ipv6 smart** command enables IPv6 return by query type.

- IPv4 to IPv6 mapping: an A query (IPv4) returns an A record
- IPv6 to IPv4 mapping: an AAAA query (IPv6) returns an AAAA record.

The **dns ipv6 smart** command disables smart mode.

Syntax

```
dns ipv6 smart
no dns ipv6 smart
```

Default Default.

Mode GSLB Policy Configuration Mode

Example These commands enables IPv6 return by query type.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns ipv6 smart
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns ipv6 smart
ACOS(config-policy:OXYGEN)#
```

Example This command disables DNS IPv6 smart mode.

```
ACOS(config-policy:OXYGEN)# no dns ipv6 smart
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns logging

Description The **dns logging** command enables DNS logging and specifies the messages that are logged.

The **no dns logging** command disables DNS logging.

Syntax

```
dns logging MESSAGE
no dns logging
```

Parameter	Description
MESSAGE	Specifies the information returned to the client. Valid options include: • **query** Query messages are logged. • **response** Response messages are logged • **both** Query and response messages are logged • **none** Neither messages are logged

Default See descriptions.

Mode GSLB Policy Configuration Mode

Example These commands enable DNS logging of neither query nor response messages.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns logging none
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns logging none
ACOS(config-policy:OXYGEN)#
```

Example This command enables DNS logging of query messages

```
ACOS(config-policy:OXYGEN)# dns logging query
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns logging query
ACOS(config-policy:OXYGEN)#
```

Example This command enables DNS logging of response messages.

```
ACOS(config-policy:OXYGEN)# dns logging response
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns logging response
ACOS(config-policy:OXYGEN)#
```

Example This command enables DNS logging of response and query messages.

```
ACOS(config-policy:OXYGEN)# dns logging both
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns logging both
ACOS(config-policy:OXYGEN)#
```

Example This command disables DNS logging.

```
ACOS(config-policy:OXYGEN)# no dns logging
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns proxy block <query>

Description The **dns proxy block <query>** command programs the ACOS Device to block DNS queries from being sent to an internal DNS server. The ACOS Device must be in GSLB proxy mode for the feature to work. The command lists the records that are blocked.

The **no dns proxy block <query>** command removes the ACOS Device's DNS query block. The command requires a record list identical to the list of records currently blocked.

Syntax

```
dns proxy block ATTRIBUTE_1 [ATTRIBUTE_2 ... ATTRIBUTE_n]
no dns proxy block ATTRIBUTES
```

Parameter	Description
ATTRIBUTE_X	Specifies information returned to the client. The command must list at least one attribute and may include more than one. Options include: • **a** • **aaaa** • **mx** • **ns** • **srv** • **cname**

Parameter	Description
	• **ptr** • **soa** • **txt** • **caa**

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands program the ACOS Device to block DNS queries with A and AAAA records.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns proxy block a aaaa
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns proxy block a aaaa
ACOS(config-policy:OXYGEN)#
```

Example This command attempts to remove A records from the list of DNS queries the ACOS Device is programmed to block.

```
ACOS(config-policy:OXYGEN)# no dns proxy block a
Field value does not match (field: a).
ACOS(config-policy:OXYGEN)#
```

Example This command removes the DNS query capacity of the ACOS Device.

```
ACOS(config-policy:OXYGEN)# no dns proxy block a aaaa
ACOS(config-policy:OXYGEN)#
```

dns proxy block <type>

Description The **dns proxy block <type>**command programs the ACOS Device to block a specified type of DNS queries. The command specifies the type, by number, of query being blocked. The device can utilize multiple command. Each command lists either a single type or a number range corresponding to multiple types.

The **no dns proxy block <type>** command restores the delivery of the specified DNS queries.

Syntax

```
dns proxy block TYPE-LIST
no dns proxy block TYPE-LIST
```

Parameter	Description
TYPE-LIST	Specifies the information returned to the client. Valid options include: • **<1-255>** Specifies a single type • **range <1-255>** Specifies a single element range of types • **range <1-255> to <1-255>** Specifies a range of types

Default See descriptions.

Mode GSLB Policy Configuration Mode (gslb policy)

Example These commands block DNS queries of type 56, 58, and 60-69.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns proxy block 56
ACOS(config-policy:OXYGEN)# dns proxy block 58
ACOS(config-policy:OXYGEN)# dns proxy block range 60 to 69
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns proxy block range 60 to 69
  dns proxy block 56
  dns proxy block 58
ACOS(config-policy:OXYGEN)#
```

Example This command removes the types 63 to 67 from the DNS query block.

```
ACOS(config-policy:OXYGEN)# no dns proxy block range 63 to 67
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns proxy block range 60 to 62
  dns proxy block range 68 to 69
  dns proxy block 56
```

```
  dns proxy block 58
ACOS(config-policy:OXYGEN)#
```

dns proxy block action

Description The **dns proxy block action** command specifies the ACOS Device method of handling blocked DNS queries.

The **no dns proxy block action** command restores the default value.

Syntax

```
dns proxy block action DISPOSITION
no dns proxy block action
```

Parameter	Description
DISPOSITION	Specifies the information returned to the client. Valid options include: • **drop** • **reject** • **ignore**

Mode GSLB Policy Configuration Mode

Example These commands

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns proxy block action drop
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns proxy block action drop
ACOS(config-policy:OXYGEN)#
```

Example This command

```
ACOS(config-policy:OXYGEN)# dns proxy block action reject
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns proxy block action reject
ACOS(config-policy:OXYGEN)#
```

Example This command

```
ACOS(config-policy:OXYGEN)# dns proxy block action ignore
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns proxy block action ignore
ACOS(config-policy:OXYGEN)#
```

Example This command

```
ACOS(config-policy:OXYGEN)# no dns proxy block action
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns selected-only

Description The **dns selected-only** command enables return of only selected IP addresses. The command specifies a limit of records that can be returned after a record is selected. When the number of records exceed the configured value, GSLB ignores this configuration.

The **no dns selected-only** command disables the return of selected IP addresses.

Syntax

```
dns selected-only [num-record]
no dns selected-only [num-record]
```

Parameter	Description
num-record	Specifies the limit of records that are returned. Valid options include: • <no parameter> – enables return of all selected records • <1-128> – specifies number of records

Default Disabled.

Mode GSLB Policy Configuration Mode

Example These commands enable the return of 32 records after receiving a query from a selected IP address.

```
ACOS(config)# gslb policy OXYGEN
```

```
ACOS(config-policy:OXYGEN)# dns selected-only 32
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns selected-only 32
ACOS(config-policy:OXYGEN)#
```

Example This command disables the return of records.

```
ACOS(config-policy:OXYGEN)# no dns selected-only 32
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

dns server

Description The **dns server** command enables a GSLB ACOS Device to act as a DNS server for specific service IPs in the GSLB zone. When this setting is enabled, the device responds directly to address queries for specific service IP addresses in the GSLB zone. The ACOS Device still forwards other types of queries to the DNS server.

The **no dns server** command disables the GSLB ACOS Device from acting as a DNS server for specific service IPs in the GSLB zone.

Syntax

```
dns serverRECORD_1 [RECORD_2 ... RECORD_N]
no dns server
```

Parameter	Description
addition-mx	Enables ACOS Device to provide the A record containing the mail server's IP address in the Additional section, when the device is configured for DNS server mode.
any	Enables ACOS Device to provide all available resource records, when the ACOS Device is configured for DNS server mode. For example, when a client issues a type "ANY" request (which is a pseudo resource record that is expressed by the wildcard code "*"), then the ACOS Device includes all RR information it has available.

Parameter	Description
any-with-metric	Provides all records with GSLB metrics applied to A/AAAA records.
authoritative	Makes the ACOS Device the authoritative DNS server for the GSLB zone, for service IPs in which *static* is enabled. If omitted,the ACOS Device is a non-authoritative DNS server for the zone domain.
caa	Provides CAA record.
cname	Allows ACOS Device to respond to inbound GSLB DNS requests that have load-balanced CNAME records.
ns [auto-ns]	Provides name server record. The **auto-ns** option automatically causes the policy to provide A records for NS records.
ptr [auto-ptr]	Provides the pointer record. The **auto-ptr** option causes the policy to provide pointer records automatically.
full-list	Appends all A records in the Authoritative section.
mx	Provides MX record in the Answer section, and A record for mail server in the Additional section, when the device is configured for DNS server mode.
naptr	Provides NAPTR record.
ns-list	This option appends all Name Server (NS) Resource Records (RR) in the Authority section of DNS replies.
sec	Provides DNSSEC support.
srv	Provides the service record.
server-mode-only	Runs GSLB in DNS server mode only.
txt	Provides the service record. TXT resource records can be used to carry multiple pieces of DNS TXT data within a single record.

Parameter	Description
zone-owner-mode	Runs GSLB in DNS server mode with zone ownership only.

Default Disabled

Mode GSLB Policy Configuration Mode

Usage When using this command, the dns cname-detect command is not required. When a client requests a configured alias name, GSLB applies the policy to the CNAME records. The **server** option is not valid with the **ip-replace** option. They are mutually exclusive.

When using this command, you also must enable the **static** option on the individual service IP. To configure the service IP addresses, use the **service-ip** command at the configuration level for the service.

Example The following commands modify the policy to program the ACOS Device to act as a DNS server for mail server and name server records.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns server ns addition-mx auto-ns
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns server addition-mx ns auto-ns
ACOS(config-policy:OXYGEN)#
```

Example The following commands disable the DNS server function on devices upon which the policy is applied.

```
ACOS(config-policy:OXYGEN)# no dns server
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

Example The following command enables the zone owner mode configuration.

```
ACOS(config-policy:OXYGEN)# dns server any authoritative zone-owner-mode
```

dns sticky

Description The **dns sticky** command programs device to send the same service IP address to a client for all requests from that client for the service address. Sticky DNS ensures that, during the aging-time, a client is always directed to the same site.

The prefix length options adjusts the granularity of the feature. The default prefix length (32 for IPv4, 128 for IPv6) causes the ACOS Device to maintain separate stickiness information for each local DNS server. For example, if two clients use DNS 10.10.10.25 as their local DNS server, and two other clients use DNS 10.20.20.99 as their local DNS server, the ACOS maintains separate stickiness information for each set of clients, by maintaining separate stickiness information for each of the local DNS servers.

When the **sticky** option is enabled, the sticky time must be at least as long as the zone TTL as defined by the ttl command at the zone configuration level. (gslb zone.)

The **no dns sticky** command restores the default value

Syntax

```
dns sticky [MASK-V4] [MASK-V6] [DURATION]
no dns sticky [MASK-V4] [MASK-V6] [DURATION]
```

Parameter	Description
MASK-V4	Specifies the IPv4 mask size. Valid options include: • <no parameter> IPv4 mask size of 32 • **/<1-32>** Specifies IPv4mask size • *dotted decimal notation* Must be valid mask value.
MASK-V6	Specifies the IPv6 mask size. Valid options include: • <no parameter> equivalent to **ipv6-mask 128** • **ipv6-mask <1-128>**
DURATION	Specifies duration limit for returning record. Valid options include:

Parameter	Description
	• <no parameter> equivalent to **aging-time 5** • **aging-time <1-65535>**

Default Disabled.
When the option is enabled, the default prefix is /32, the default aging time is 5 minutes, and the default IPv6 mask length is 128.

Mode GSLB Policy Configuration Mode (gslb policy)

Usage If more than one of the following options are enabled, GSLB uses them in the order listed:

1. **sticky**
2. **server**
3. **cache**
4. **proxy** (The command does not have a separately configurable "proxy" option. The proxy option is automatically enabled when you configure the DNS proxy.)

The site address selected by the first option that is applicable to the client and requested service is used.

Example These commands enables DNS sticky and establishes default values for aging time and the masks.

```
ACOS(config)# gslb policy NEON
ACOS(config-policy:NEON)# dns sticky
ACOS(config-policy:NEON)# show run | sec gslb
gslb policy NEON
  dns sticky
ACOS(config-policy:NEON)#
```

Example This command configures non-default values for the aging time and masks.

```
ACOS(config-policy:NEON)# dns sticky /30 aging-time 15 ipv6-
mask 124
ACOS(config-policy:NEON)# show run | sec gslb
gslb policy NEON
  dns sticky /30 ipv6-mask 124 aging-time 15
```

```
ACOS(config-policy:NEON)#
```

Example This command modifies IPv4 mask size without changing the other parameters.

```
ACOS(config-policy:NEON)# dns sticky /24 aging-time 15 ipv6-
mask 124
ACOS(config-policy:NEON)# show run | sec gslb
gslb policy NEON
  dns sticky /24 ipv6-mask 124 aging-time 15
ACOS(config-policy:NEON)#
```

Example This command explicitly changes the parameter values to their defaults.

```
ACOS(config-policy:NEON)# dns sticky /32 ipv6-mask 128 aging-
time 5
ACOS(config-policy:NEON)# show run | sec gslb
gslb policy NEON
  dns sticky
ACOS(config-policy:NEON)#
```

Example This command disables DNS sticky

```
ACOS(config-policy:NEON)# no dns sticky
ACOS(config-policy:NEON)# show run | sec gslb
gslb policy NEON
ACOS(config-policy:NEON)#
```

dns sticky option

Description The **dns sticky option** command programs GSLB device to configure specific behaviors related to sticky session creation. Sticky DNS option ensures that a client is always directed to the same site or server by utilizing EDNS Client Subnet (ECS) information.

When the **edns-client-subnet** option is enabled, it allows the GSLB to use ECS data for creating a sticky session.

Syntax

```
dns sticky-option
edns-client-subnet
edns-client-subnet only
```

Default Disabled.

Mode GSLB Policy Configuration Mode (gslb policy)

Usage This command is optional for configuring sticky session in GSLB system. By using ECS, it allows the system to provide an additional protection by masking the client's real source IP.

Example These commands enable DNS sticky-options with EDNS client subnet and establish default values for aging time and the masks.

```
ACOS(config)# gslb policy NEON
ACOS(config-policy:NEON)# dns sticky
ACOS(config-policy:NEON)# dns sticky-options
ACOS(config-policy:NEON-sticky-options)# edns-client-subnet
ACOS(config-policy:NEON-sticky-options)# show run | sec gslb
gslb policy NEON
  dns sticky
  dns sticky-options
      edns-client-subnet
ACOS(config-policy:NEON)#
```

Example These commands enable DNS sticky-options with EDNS client subnet only and establish default values for aging time and the masks.

```
ACOS(config)# gslb policy NEON
ACOS(config-policy:NEON)# dns sticky
ACOS(config-policy:NEON)# dns sticky-options
ACOS(config-policy:NEON-sticky-options)# edns-client-subnet
only
ACOS(config-policy:NEON-sticky-options)# show run | sec gslb
gslb policy NEON
  dns sticky
  dns sticky-options
      edns-client-subnet only
ACOS(config-policy:NEON)#
```

Example These commands enable DNS sticky with EDNS client subnet and establish non default values for aging time.

```
ACOS(config)# gslb policy NEON
ACOS(config-policy:NEON)# dns server srv txt any server-mode-
only
ACOS(config-policy:NEON)# dns sticky /32 aging-time 10
```

```
ACOS(config-policy:NEON)# dns sticky-options
ACOS(config-policy:NEON-sticky-options)# edns-client-subnet
ACOS(config-policy:NEON-sticky-options)# show run | sec gslb
gslb policy NEON
 dns server srv txt any server-mode-only
  dns sticky /32 aging-time 10
  dns sticky-options
      edns-client-subnet
ACOS(config-policy:NEON)#
```

dns ttl

Description The **dns ttl** command programs the ACOS Device to change the TTL of each DNS record in DNS replies received from the DNS for which the device is a proxy.

The **dns use-server-ttl** command programs the device to use the time-to-live value in the DNS server response instead of replacing it with a specified value.

The **no dns ttl** and **no dns use-server-ttl** command restores the default value of 10 seconds. The latter command is available only when **dns use-server-ttl** is configured.

Syntax

```
dns ttl DURATION
dns use-server-ttl
no dns ttl
dns use-server-ttl
```

Parameter	Description
DURATION	Specifies the new TTL value (seconds). Value ranges from 0 to 1000000000 (one billion).

Default 10 seconds.

Mode GSLB Policy Configuration Mode

Example These commands program the device to change TTL for DNS replies to 30 secs.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns ttl 30
```

```
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns ttl 30
ACOS(config-policy:OXYGEN)#
```

Example This command programs the device to use TTL from DNS records in DNS replies.

```
ACOS(config-policy:OXYGEN)# dns use-server-ttl
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
  dns use-server-ttl
ACOS(config-policy:OXYGEN)#
```

Example This command programs the device to change TTL for DNS replies to 10 seconds.

```
ACOS(config-policy:OXYGEN)# no dns ttl
ACOS(config-policy:OXYGEN)# show run | sec gslb
gslb policy OXYGEN
ACOS(config-policy:OXYGEN)#
```

edns client-subnet geographic

Description Use the EDNS-Client-Subnet field for GSLB geo-location metric.

For DNS queries, not all requests use a third-party resolver that is in close topographical proximity to themselves. Some recursive resolvers use an extra EDNS field in DNS messages to forward details about where a network query is coming from. ACOS can read the extra EDNS-Client-Subnet field and provide more specific topological geo-location features for DNS queries in GSLB.

When enabled, the information in the EDNS-Client-Subnet field will be checked against the configured geo-location database first. If the extra field contains no information, then ACOS will check the source IP of the recursive DNS server against the configured geo-location database in order to perform GSLB geo-location metric. As back-end servers can also generate an OPT resource record, ACOS can read EDNS-Client-Subnet fields from responses as well.

ACOS uses ENDS-Client-Subnet in GSLB server mode. Proxy mode is not supported.

Syntax `[no] edns client-subnet geographic`

Default Disabled.

Mode GSLB Policy

Usage This command allows ACOS to read the extra field in DNS messages, and to provide more specific topological geo-location features for DNS queries, based on the client's subnet. The information in the EDNS field is checked against configured geo-location databases first.

Example This example configures a device to read EDNS-Client-Subnet field in DNS queries. In the example, if client traffic comes in with a source IP 11.11.11.11, but the EDNS-Client-Subnet is 10.10.10.10, the DNS A record vs1 is selected because the client's EDNS-Client-Subnet corresponds to the geo-location of site1. The EDNS-Client-Subnet 10.10.10.10 will be used for all geo-location metric features.

These commands configure two user-defined geo-locations.

```
ACOS(config)# gslb geo-location site1
ACOS(config-geo-location:site1)# ip 10.10.10.10 mask /24
ACOS(config-geo-location:site1)# exit
ACOS(config)# gslb geo-location site2
ACOS(config-geo-location:site2)# ip 11.11.11.11 mask /32
ACOS(config-geo-location:site2)# exit
```

The following commands configure example GSLB sites and their respective geo-locations and SLB servers with virtual servers.

```
ACOS(config)# gslb site usa
ACOS(config-gslb site:usa)# geo-location site1
ACOS(config-gslb site:usa)# slb-dev acos1 10.10.10.10
ACOS(config-gslb site:usa-slb dev:acos1)# vip-server vs1
ACOS(config-gslb site:usa-slb dev:acos1)# exit
ACOS(config-gslb site:usa)# exit
ACOS(config)# gslb site china
ACOS(config-gslb site:china)# geo-location site2
ACOS(config-gslb site:china)# slb-dev acos2 200.20.20.20
ACOS(config-gslb site:china-slb dev:acos2)# vip-server vs2
```

```
ACOS(config-gslb site:china-slb dev:acos2)# exit
ACOS(config-gslb site:china)# exit
```

These commands configure an example GSLB policy related to DNS traffic.

```
ACOS(config)# gslb policy dns
ACOS(config-policy:dns)# dns selected-only
ACOS(config-policy:dns)# dns server authoritative
ACOS(config-policy:dns)# edns client-subnet geographic
ACOS(config-policy:dns)# exit
```

The following commands configure an example GSLB zone for example.com.

```
ACOS(config)# gslb zone example.com
ACOS(config-zone:example.com)# policy dns
ACOS(config-zone:example.com)# service 80 http
ACOS(config-zone:example.com-service:http)# exit
ACOS(config-zone:example.com)# service 80 www
ACOS(config-zone:example.com-service:www)# dns-a-record vs1
static
ACOS(config-zone:example.com-service:www)# dns-a-record vs2
static
```

geo-location

Description Configure a geographic location. GSLB forwards client requests from IP addresses within the location's range to the GSLB site that serves the location.

Syntax

```
[no] geo-location location-name
```

This command takes you to the geo-location configuration level within a GSLB policy, where the following options are available:

Command	Description
ip *start-ipv4-addr* {mask *ipv4-mask* | *end-ipv4-addr*}	Specify the beginning IP address and subnet mask or ending IP address for an IPv4 address range.

Command	Description
ipv6 *start-ipv6-addr* {**mask** *ipv6-mask* | *end-ipv6-addr*}	Specify the beginning IP address and subnet mask or ending IP address for an IPv6 address range.

Default None.

Mode GSLB Policy

Usage To prefer the location configured with this command over a globally configured location, use the command geo-location-match.

Example The following example configures geographic location “CN.BeiJing” for IP address range 200.1.1.1 through 200.1.1.253:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# geo-location CN.Beijing
ACOS((config-policy:pol1-geo-location:CN.B...)# ip 200.1.1.1
200.1.1.253
```

geo-location-match

Description Configure the policy to prefer either the globally configured geo-location or the one configured in this policy. If a client IP address matches the IP ranges in a globally configured location and in a location configured in this policy, the **geo-location match-first** command specifies which matching geo-location to use.

Syntax

```
[no] geo-location-match
{match-first {global | policy} | overlap [global | policy]}
```

Parameter	Description
match-first {**global** | **policy**}	Configure policy to prefer either the globally configured geo-location or the one configured in the policy. If a client IP address matches IP ranges in a globally configured location and in a location configured in the policy, the command specifies the geo-location that is used.

Parameter	Description
	• **global** - GSLB prefers globally configured locations. • **policy** - GSLB prefers locations configured in this policy. The default is **global**.
overlap [**global** | **policy**]	Enabled overlap matching mode. If there are overlapping addresses in the geo-location database, use this option to enable the ACOS Device to find the most precise match. • **global** - GSLB prefers globally configured locations. • **policy** - GSLB prefers locations configured in this policy.. The default is **global**.

Default See descriptions.

Mode GSLB Policy

Usage If you suspect a public IP address in your domain is not unique and the same IP address may be associated with different hosts, you can enable the geo-location overlap option. This causes the ACOS Device to search the geo-location database for the match best (or longest matching IP address). Otherwise, the ACOS Device will use its default behavior, which is to scan the specified geo-location database using the “match first” algorithm, which uses the first IP address-region mapping discovered.

Example The following command configures the GSLB controller to prefer locations configured in this policy:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# geo-location-match match-first
policy
```

geographic

Description Enable or disable the Geographic metric. The Geographic metric prefers sites that are within the geographic location of the client.

Syntax

```
[no] geographic
```

Default Enabled

Mode GSLB Policy

Usage You must configure the geographic location, by configuring a geo-location name, then assigning the gslb geo-location to a gslb site. To configure a geo-location, assign a client IP address range to a location name. To assign the geo-location to a site, use the geo-location command at the site configuration level.

Example The following command disables the Geographic metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no geographic
```

health-check

Description Enable or disable the Health-Check metric. The Health-Check metric prefers sites that pass their health checks.

Syntax

```
[no] health-check
```

Default Enabled

Mode GSLB Policy

Usage This metric requires the GSLB protocol to be enabled both on the GSLB controller and site ACOS Devices, *if the default health checks are used on the service IPs*.

If you use a custom health monitor, or you explicitly apply the default Layer 3 health monitor to the service, the GSLB protocol is not used for any of the health checks. In this case, the GSLB protocol is not required to be enabled on the site ACOS Devices, although use of the protocol is still recommended.

Example The following command disables the Health-Check metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no health-check
```

ip-list

Description Use an IP list to exclude a set of IP addresses from aRDT polling.

Syntax

```
[no] ip-list list-name
```

Default None

Example The following commands configure a GSLB IP list and use the list to exclude IP addresses from an RDT data collection:

```
ACOS(config)# gslb ip-list iplist1
ACOS(config-ip list:iplist1)# ip 192.168.1.0 /24 id 3
ACOS(config-ip list:iplist1)# ip 10.10.10.10 /32 id 3
ACOS(config-ip list:iplist1)# ip 10.10.10.20 /32 id 3
ACOS(config-ip list:iplist1)# ip 10.10.10.30 /32 id 3
ACOS(config-ip list:iplist1)# exit
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# ip-list iplist1
ACOS(config-policy:pol1)# active-rdt ignore-id 3
```

Related Commands:

- gslb ip-list

least-response

Description Enable or disable the Least-Response metric, which prefers VIPs that have the fewest hits.

Syntax

```
[no] least-response
```

Default Disabled

Mode GSLB Policy

Example The following command enables the Least-Response metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# least-response
```

metric-fail-break

Description Enable GSLB to stop if there are no valid service IPs.

Syntax

```
[no] metric-fail-break
```

Default Disabled

Mode GSLB Policy

metric-force-check

Description Force the GSLB controller to always check all metrics in the policy.

Syntax

```
[no] metric-force-check
```

Default By default, the GSLB controller stops evaluating metrics for a site once a metric comparison definitively selects or rejects a site.

Mode GSLB Policy

metric-order

Description Configure the order in which the GSLB metrics in this policy are used.

Syntax

```
[no] metric-order metric [metric ...]
```

Parameter	Description
metric [*metric ...*]	One or more of the following metrics: • **active-rdt** • **active-servers** • **admin-ip** • **admin-preference** • **bw-cost** • **capacity** • **connection-count-by-site** • **connection-load**

Parameter	Description
	• **geographic** • **health-check** • **least-response** • **num-session** • **weighted-ip** • **weighted-site**

Default The Health-Check, Geographic, and Round-Robin metrics are enabled by default. The Round-Robin metric does not appear in the list above because this is the metric of last resort.

Mode GSLB Policy

Usage The first metric you specify with this command becomes the primary metric. If you specify additional parameters, they are used in the priority you specify. All remaining metrics are prioritized to follow the metrics you specify.

The GSLB Controller uses each metric, in the order specified, to compare the IP addresses returned in DNS replies to clients. If a metric is disabled, the metric order does not change. The GSLB Controller skips the metric and continues to the next enabled metric.

The Round-Robin metric can not be re-ordered.

To view the metric order used in a policy, see show gslb policy.

num-session

Description Configure the Num-Session metric, which evaluates a site based on available session capacity and tolerance threshold compared to another site. Sites that are at or below their thresholds of current available sessions are preferred over sites that are above their thresholds.

When dealing with smaller base numbers, a small fluctuation in the number of available sessions can cause flapping from one site to another. Thus, when configuring sites with smaller capacities, it is

recommended to use a larger tolerance number to prevent frequent flapping between preferred sites.

Example Site A has 800,000 sessions available and Site B has 600,000 sessions available. If Num-Session is enabled, then Site A is preferred because it has a larger number of available sessions than site B.

If the tolerance option is enabled (with a default value of 10 percent), and if Site A has 800,000 sessions available and Site B has 600,000 sessions available, then Site A will continue to be preferred until Site B's available sessions exceed Site A's available sessions by more than 10 percent. In this case, Site A will remain the preferred site until Site B's available sessions exceed 800,000 by more than ten percent (or 80,000 sessions). If Site A's available sessions remain constant, and Site B's available sessions increase to the point that they exceed 880,000 sessions, the Site B would become the preferred site.

Syntax

```
num-sessiontolerance num
```

The tolerance number is a number from 0 to 100 specifying the percentage by which the number of available sessions on site SLB devices can differ without causing the Num-Session metric to select one site device over another.

The **num-session tolerance** command has no negative form. To reset the Num-Session tolerance back to default, enter the following command, which changes the Num-Session tolerance back to the default percentage:

```
num-session tolerance 10
```

NOTE: Use the num-session-enable command to enable or disable the Num-Session metric.

Default Disabled.

The default tolerance is 10 percent.

Mode GSLB Policy

Usage The GSLB ACOS Device considers site SLB devices to be equal if the difference in the number of available sessions on each device does not

exceed the tolerance percentage. The tolerance percentage ensures that minor differences in available sessions do not cause frequent, unnecessary, changes in site preference.

This metric requires the GSLB protocol to be enabled both on the GSLB controller and on the site ACOS Devices.

Example The following command changes the available-session tolerance threshold to 70 percent:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# num-session-enable
ACOS(config-policy:pol1)# num-session tolerance 70
```

num-session-enable

Description Enable or disable the Num-Session metric.

Syntax

```
[no] num-session-enable
```

Default Disabled

Mode GSLB Policy

Example The following command changes the available-session tolerance threshold to 70 percent:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# num-session-enable
ACOS(config-policy:pol1)# num-session tolerance 70
```

round-robin

Description Configure the Round-Robin metric, which selects sites in sequential order.

Syntax

```
[no] round-robin
```

Default Enabled

Mode GSLB Policy

Usage The ACOS Device uses Round-Robin to select a site at the end of the policy parameters evaluation. This is true even if the Round-Robin metric is disabled in the GSLB policy.

Example The following command disables the Round-Robin metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no round-robin
```

weighted-alias

Description Enable the Weighted Alias metric, which prefers CNAME records with higher weight values over CNAME records with lower weight values. This metric is similar to Weighted-IP, but applies only to DNS CNAME records.

Syntax

```
[no] weighted-alias
```

Default Disabled

Mode GSLB Policy

Usage Metric order does not apply to this metric.

To configure the Weighted Alias metric:

1. At the configuration level for the GSLB service, use the **weight** command to assign a weight to the DNS CNAME record for the service.
2. At the configuration level for the GSLB policy:
   - Enable the Weighted Alias metric.
   - Enable one or both of the following DNS options, as applicable to your deployment:
   - DNS backup-alias
   - DNS geoloc-alias
3. If using the backup-alias option, use the **dns-cname-record as-backup** option on the service.

Related Commands:

- gslb service-ip

weighted-ip

Description Configure the Weighted-IP metric, which uses service IP addresses with higher weight values more often than addresses with lower weight values.

Syntax

```
[no] weighted-ip total-hits
```

The **total-hits** option will send requests to the service IP addresses that have fewer hits first. After all service IP addresses have the same number of hits, GSLB sends requests based on weight. This option is disabled by default.

Use the weighted-ip-enable command to enable selection of the Service-Ip by weighted preference.

Default Disabled

Mode GSLB Policy

Usage As a simple example, assume that the Weighted-IP metric is the only enabled metric, or at least always ends up being used as the tie breaker. The **total-hits** option is disabled. IP address 10.10.10.1 has weight 4 and IP address 10.10.10.2 has weight 2. During a given session aging period, the first 4 requests go to 10.10.10.1, the next 2 requests go to 10.10.10.2, and so on, (4 to 10.10.10.1, then 2 to 10.10.10.2).

Here is an example using the same two servers and weights, with the **total-hits** option enabled. IP address 10.10.10.1 has weight 4 and total hits 8, and IP address 10.10.10.2 has weight 2 and total hits 0. In this case, the first 4 requests go to 10.10.10.2, then the requests are distributed according to weight. Four requests go to 10.10.10.1, then two requests go to 10.10.10.2, and so on. To display the total hits for a service IP address, use the gslb service-ip command.

To assign a weight to a service IP address, use the following command at the configuration level for the zone service:

dns-a-record *name* **weight** *num*

Example The following command disables the Weighted-IP metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no weighted-ip-enable
```

weighted-ip-enable

Description Enable selection of the Service-Ip by weighted preference.

Syntax

```
[no] weighted-ip-enable
```

Default Disabled

Mode GSLB Policy

Example The following command disables the Weighted-IP metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no weighted-ip-enable
```

weighted-site

Description Configure the Weighted-Site metric, which uses sites with higher weight values more often than sites with lower weight values.

Syntax

```
[no] weighted-site total-hits
```

The **total-hits** option will send requests to the service IP addresses that have fewer hits first. After all service IP addresses have the same number of hits, GSLB sends requests based on weight. This option is disabled by default.

Use weighted-site-enable command to enable selection of the Service-IP by weighted preference.

Default Disabled. When Weighted-Site metric is enabled, default weight of each site is 1.

Mode GSLB Policy

Usage As a simple example, assume that the Weighted-Site metric is the only enabled metric, or at least always ends up being the tie breaker. Site A has weight 4 and site B has weight 2. During a given session aging period, the first 4 requests go to site A, the next 2 requests go to site B, and so on, (4 to A, then 2 to B).

This example uses the same two sites and weights, with the **total-hits** option enabled: Site A has weight 4 with total hits 8; site B has weight 2 with total hits 0. In this case, the first 4 requests go to site B, then

requests are sent as described above. Four requests go to site A, then 2 requests go to site B, and so on.

To assign weight to a site, use the **weight** command.

Example The following command disables the Weighted-Site metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no weighted-site-enable
```

weighted-site-enable

Description Enable selection of the Service-IP by weighted preference.

Syntax

```
[no] weighted-site-enable
```

Default Disabled

Mode GSLB Policy

Example The following command disables the Weighted-Site metric:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# no weighted-site-enable
```

dns server

Description GSLB server-mode returns all service-ip for all records. The command option

Syntax

```
dns server {any | any-with-metric}
```

Parameters	Description
any	Specify this option to view all service-ip for all records by default and the records are sent based on the health check configurations.
any-with-metric	Specify to get metric details with an “any” query.

Default “any”

Mode GSLB Server Mode

Usage The "dns server any" and "dns server any-with-metric" options cannot be used together, as they are mutually exclusive.

Example

```
ACOS(config)# dns server any
ACOS(config)# dns server any-with-metric
```

gslb protocol

Description Enable the GSLB protocol, set protocol or SSL options.

Syntax

```
[no] gslb protocol
{
msg-format-acos-2x |
auto-detect |
enable {controller | device} |
limit option |
ping [site | ip-addr] |
status-intervalseconds |
use-mgmt-port |
secure {disable | enable-fallback | enable}
}
```

Parameter	Description
msg-format-acos-2x	Enables GSLB message format compatibility for ACOS 2.x versions.
auto-detect	Enables auto-detection. This is disabled by default.
enable {**controller** | **device**}	Enables the GSLB protocol: • controller – Use this option on the ACOS Device on which GSLB is configured. • device – Use this option on the ACOS Devices that are SLB devices at the GSLB sites.
limit *option*	See gslb protocol limit.
ping	Test GSLB connectivity from the GSLB ACOS Device to

Parameter	Description
[site | ip-addr]	a site ACOS Device. • site - GSLB site name of the site ACOS Device. • ip-addr - The IP address of the site ACOS Device.
status-interval *seconds*	Changes the number of seconds between GSLB status messages. You can specify 1-1800 seconds. The default is 30 seconds.
use-mgmt-port	Use the management route table instead of the data route table. This is disabled by default.
secure enable	Enable secure SSL GSLB protocol. This is default configuration, and supports SSL. When enable is configured, then it only connects to peers that also support SSL.
secure disable	Disable secure SSL GSLB protocol. If this command is run on the controller at the first open message, protocol is disabled on all connected GSLB devices.
secure enable-fallback	Enable fall back option for the GSLB protocol where configuration falls back to non-secure if the SSL connection fails. ACOS enables SSL on the GSLB controller. If the GSLB peer doesn't support SSL, then ACOS falls back to regular TCP plain text.

NOTE: For the **limit** options, see gslb protocol limit.

Default See descriptions.

Mode Global configuration mode

Usage The GSLB protocol uses port 4149 and is registered on this port for both TCP and UDP.

The secure GSLB option provides option to enable or disable SSL for GSLB protocol.

ACOS Devices use the GSLB protocol for GSLB management traffic. The protocol must be enabled on the GSLB controller, and it is recommended (but not required) that you enable the protocol on the site ACOS Devices.

The following GSLB policy metrics require the protocol to be enabled on both the site ACOS Devices as well as the GSLB controller:

- Session-Capacity
- aRDT
- Connection-Load
- Num-Session

The GSLB protocol is also required for the health-check metric, if the default health checks are used. If you modify the health checks, the GSLB protocol is not required.

Example The following command enables the GSLB protocol on a GSLB device:

```
ACOS(config)# gslb protocol enable controller
```

Example The following command enables the GSLB protocol on a site device:

```
ACOS(config)# gslb protocol enable device
```

Example The following command enables the GSLB message format compatibility with ACOS 2.x versions.

```
ACOS(config)# gslb protocol msg-format-acos-2x
```

Example The following command enables, disables SSL for GSLB protocol, or falls back to non-secure GSLB on a site device.

```
ACOS(config)# gslb protocol secure enable
ACOS(config)# gslb protocol secure enable-fallback
ACOS(config)# gslb protocol secure disable
```

gslb protocol limit

Description Change aRDT message limits.

Syntax

```
[no] gslb protocol limit
{
```

```
ardt-query num-msgs |
ardt-response num-msgs |
ardt-session num-sessions |
conn-response num-msgs |
message num-msgs |
response num-msgs
}
```

Parameter	Description
ardt-query	Limits the number of aRDT Query messages (0-1000000). The default is 200 query messages.
ardt-response	Limits the number of aRDT Response Messages (0-1000000). The default is 1000 response messages.
ardt-session	Limits the number of aRDT sessions (0-1000000) The default is 32768 sessions.
conn-response	Limits the number Connection Load Response Messages (0-1000000). By default no limit is set.
message	Limits the number of messages (0-1000000). The default is 10000 (ten thousand) messages.
response	Limits the number of Response Messages (0-1000000). The default is 3600 response messages.

Default See descriptions.

Mode Global configuration mode

gslb secure-attributes

Description Configure attributes for secure GSLB connection. The above configuration we can configure, cert-key pair to be used for SSL handshake. This is also per-partition.

The cert and key used in this configuration, should already exist on the box, which are brought using existing PKI commands. (pki create cert, import cert, import key)

Syntax

```
gslb secure-attributes {cert <cert_name> key <key_name> |
enable | disable | enable-fallback | }
```

Parameter	Description
secure attributes	Define secure attributes like SSL certificates and related configuration.
cert *<cert_ name>*	Specify SSL certificate for secure GSLB. Maximum length of certificate name 245 characters.
key *<key_ name>*	Specify SSL key name for secure GSLB. Maximum length of key name 245 characters.
enable	Enable secure GSLB.
disable	Disable secure GSLB.
enable-fallback	Fallback to non-secure GSLB if there is no secure GSLB connection.

Default Check the syntax descriptions

Mode Configure Secure Attributes mode

Usage If GSLB is configured per partition, it has priority over global configuration for that particular partition. By default it is set to **use-global-config**, to follow the behaviour configured globally under "**gslb protocol secure**" in shared partition.

Example The following commands displays how to configure secure attributes:

```
ACOS (config)# gslb secure-attributes
ACOS (config-secure-attributes)# cert cert_ssl key ssl_1
ACOS (config-secure-attributes)# enable-fallback
ACOS (config-secure-attributes)# enable
ACOS (config-secure-attributes)# disable
```

gslb service-group

Description Configure an FQDN group.

Syntax

```
[no] gslb service-group group-name
```

This command creates the group and changes the CLI to the configuration level for it. At this level, the following commands are available:.

Parameter	Description
[no] dependency site	All services become unavailable on the site when one service goes down. Facilitates traffic redirection to a site that can maintain persistence for all services. Default setting is disabled. Only valid when `persistent site` is enabled.
[no] disable	Disables all FQDN members.
[no] disable-site *site-name*	Disables the given site name in the service-group.
[no] persistent site [*AGE*] [*V4*] [*V6*]	Enables site persistence for the configuration mode service group. Parameter options include: • ***AGE*** – Specifies enforcement period. Valid options include: ◦ <no parameter> – default period of five minutes. ◦ `aging-time <1-65535>` – specifies period (minutes) • ***V4*** – Specifies IPv4 mask. Valid formats include: ◦ <no parameter> – IPv4 mask of /32. ◦ /nn – specifies IPv4 mask length ◦ A.B.C.D – must specify valid IPv4 mask

Parameter	Description
	• *v6* – Specifies IPv6 mask length. Valid formats include: ◦ <no parameter> – default IPv6 mask of 128. ◦ `ipv6-mask <1-128>` – specifies IPv6 mask length
`[no] member` *service-name.zone-name*	Adds the specified service, in FQDN format.

Example These commands 1) create an FQDN; 2) create an FQDN group called "example-group"; and 3) adds the FQDN for GSLB services to the group:

```
ACOS(config)# gslb zone example.com
ACOS(config-zone:example.com)# service 80 www
ACOS(config-zone:example.com-service:www)# exit
ACOS(config-zone:example.com)# exit
ACOS(config)# gslb service-group example-group
ACOS(config-svc group:example-group)# member www.example.com
ACOS(config-svc group:example-group)# member www1.example.com
```

gslb service-ip

Description Configure a service IP, which can be a virtual server's or real server's IP address.

Syntax

```
[no] gslb service-ip service-name [ipaddr]
```

Parameter	Description
service-name	Name of the service, up to 63 alphanumeric characters.
ipaddr	IP address of the virtual server or real server. You can specify an IPv4 or IPv6 address. (If you are changing the configuration of a GSLB service that is already configured, this parameter is not required.)

This command changes the CLI to the configuration level for the specified service, where the following GSLB-related commands are available:

Command	Description
disable	Disables GSLB for the service IP address.
enable	Enables GSLB for the service IP address.
[**no**] **external-ip** *ipaddr*	Assigns an external IP address to the service IP. The external IP address allows a service IP that has an internal IP address to be reached from outside the internal network.
[**no**] **health-check** *monitor-name*	Configures service IP monitoring. If you enter the command with no options, the default Layer 3 health monitor (ICMP ping) is used. *monitor-name* – The service is checked using the specified Layer 3, 4 or 7 health monitor.
[**no**] **health-check-disable**	Disables the health-check monitor.
[**no**] **health-check-protocol-disable**	Disables the GSLB protocol health monitor.
[**no**] **ipv6** *ipv6-addr*	Maps the specified IPv6 address to an IPv4 service IP. This option also requires IPv6 DNS AAAA support to be enabled in the GSLB policy. (See the **ipv6-mapping** option in dns ipv6 mapping.)
[**no**] **port** *num* [**tcp** | **udp**] [**port-service-name**]	Adds base service port to the service IP. The ports can be TCP or UDP. • **disable** – Disables GSLB server port. • **enable** – Enables GSLB server port. • **[no] health-check** [*monitor-name*] – Enables

Command	Description
	health monitoring for the server port. If you do not specify a health monitor, the default health monitor is used. (See "Usage" below.) • **`[no] health-check-disable`** – Enables or disables health monitoring for server port. • **`[no] health-check-follow-port`** – Specify the port to follow for health status. The port cannot follow itself or use port 0. • **`[no] health-check-protocol-disable`** – Disable the GSLB protocol health monitor for the server port. Additionally, you can define a name for a service or application that is running on this port. Multiple services can be defined for different applications, such as, HTTP or FTP. For example, `port 80 tcp http`. Here, `http` service is running on port 80. You can also bind health checks to the individual service port for monitoring its status. • ***`port-service-name`*** – Define a name for the port service. The length of the port service name can be upto 64 characters. This command changes the CLI to the configuration level for the specified service port, where the following GSLB-related commands are available: ◦ **`disable`** – Disables GSLB service port. ◦ **`enable`** – Enables GSLB service port. ◦ **`[no] health-check`** *`[monitor-name]`* – Enables health monitoring for the service port. If you do not specify a health monitor, the default health monitor is used. (See "Usage" below.)

Command	Description
	○ **[no] health-check-disable** – Enables or disables health monitoring for service port. ○ **[no] health-check-protocol-disable** – Disable the GSLB protocol health monitor for the service port.

Default No services are configured by default. When you configure a service, the service is enabled by default, and the default port is 80. The default health monitor for a service is the default Layer 3 health monitor (ICMP ping). The default health monitor for a service port is the default TCP or UDP monitor, depending on the transport protocol. (For more on health checking, see "Usage" below.)

Mode Global configuration mode

Usage If you leave the health monitor for a service at its default setting (the default ICMP ping health check), health checks are performed within the GSLB protocol.

If you use a custom health monitor, or explicitly apply the default Layer 3 health monitor to the service, the GSLB protocol is not used for any of the health checks.

If you use a custom health monitor for a service port, the port number specified in the service configuration is used instead of the port number specified in the health monitor configuration.

The following policy metric options are not supported for IPv6 service IPs:

- active-rdt
- ip-list
- dns external-ip
- dns ipv6 mapping
- geo-location

Example The following example creates a GSLB service IP address named "gslb-srvc2" with IP address 192.160.20.99:

```
ACOS(config)# gslb service-ip gslb-srvc2 192.168.20.99
ACOS(config-service-ip:gslb-srvc2)#
```

Example The following example creates the 'http and 'gitlab' labels for services under service-ip port 80 tcp.

```
ACOS(config)# gslb service-ip s1 10.20.20.30
ACOS(config-service-ip:s1)# service 80 tcp http
ACOS(config-service-ip:s1-service:http)# health-check-
protocol-disable
ACOS(config-service-ip:s1-service:http)# exit
ACOS(config-service-ip:s1)# service 80 tcp gitlab
ACOS(config-service-ip:s1-service:gitlab)# health-check-
protocol-disable
ACOS(config-service-ip:s1-service:gitlab)# exit
ACOS(config-service-ip:s1)# port 80 tcp
ACOS(config-service-ip:s1)# port 53 udp
ACOS(config-service-ip:s1)# exit
```

gslb service-matching-rules

Description Configure service matching rules in the GSLB zone to redirect DNS queries based on certain conditions.

Syntax

```
[no] gslb service-matching-rules zone zone-name
```

Parameter	Description
zone-name	Specify the name of the GSLB zone where the service matching rules need to be configured. You can enter a zone name containing up to 127 alphanumeric characters.

This command changes the CLI to the configuration level for the specified zone, where the following sub-commands are available:

Command	Description
[no] disable	Disable rule matching for the associated

Command	Description
	zone.
[no] hitcount-enable	Configure this option to enable the hit count for rule matching. You can view these counters using the show gslb zone service-matching-rules command. This parameter is disabled by default.
[no] rule *num*	Configure a service matching rule by specifying a rule number between 1 and 500. This number also determines the sequence in which the rules are matched, starting with rule 1 and ending with rule 500. **NOTE:** You can configure up to 500 service matching rules in one GSLB zone.

The **rule** command changes the CLI to the configuration level for the rule, where the following sub-commands are available:

Command	Description
domain-name { equals | contains | starts-with | ends-with } *domain-name*	Match the rule based on the domain name by checking if the DNS query name matches the specified domain name string (1-255 characters). The following match-options are available: • **equals** - Matches only if the domain name completely matches the specified string. • **contains** - Matches if the specified string appears anywhere within the domain name. • **starts-with** - Matches only if the

Command	Description
	domain name starts with the specified string. • **ends-with** - Matches only if the domain name ends with the specified string. **NOTE:** The domain name string matching is case-insensitive.
health-state { gslb-site *site-name* **| gslb-service-ip** *service-ip-name* **| slb-server** *server-name*}	Match the rule based on the health state of the specified object. Specify one or more from the following objects along with the corresponding states: • **gslb-site** *gslb-site-name* - The GSLB site name (1-63 characters) to be matched. Specify one of the following states: ◦ **AllUp** - All components of the specified GSLB site are up and running. ◦ **AllUp-or-PartUp** - All or at least one component of the specified GSLB site is up and running. ◦ **Down-or-PartUp** - The specified GSLB site is either completely down or only partially up. ◦ **Down** - All components of the specified GSLB site are down. • **gslb-service-ip** *gslb-service-ip-name* - The GSLB service IP name (1-63 characters) to be matched. Specify one of the following states:

Command	Description
	◦ **Up** - The specified GSLB service IP is up, operational, and reachable. ◦ **Down** - The specified GSLB service IP is down and not operational. • **slb-server** *slb-server-name* - The SLB server name (1-127 characters) to be matched. Specify one of the following states: ◦ **Up** - The specified SLB server is up and operational. ◦ **Down** - The specified SLB server is down and not operational. **NOTE:** You can configure maximum of 4 health state conditions.
source-addr { *A.B.C.D/nn* **|** *A:B:C:D:E:F:G:H/nn* **}**	Match the rule based on the client source IP address by checking if it falls within the specified subnet. Specify the subnet using one of the following formats: • *A.B.C.D/nn* - IPv4 subnet • *A:B:C:D:E:F:G:H/nn* - IPv6 subnet
service *zone-service-name*	Specify the service name (1-63 characters) within the GSLB zone where the DNS query should be redirected after the rules are matched.

Default There are no rules configured by default.

Mode Global configuration mode

Usage

A service matching rule allows you to redirect DNS queries to a target zone service based on specific conditions, such as the domain name, the client's source IP, and the health status of GSLB service IP, GSLB site, or SLB server.

When a client DNS query is received, if it matches all the conditions in a service matching rule, the query is redirected to the configured target service of the matched rule (under the same zone). The policies and configurations of the new target service are then used to process the query.

Example

The following example creates two service matching rules within the GSLB zone *a10.com*. If the conditions from **rule** *1* match, the DNS query is redirected to *www-view-cl1*. Else, if the conditions from **rule** *2* match, the query is redirected to *www-view-cl2*:

```
ACOS(config)# gslb service-matching-rules zone a10.com
ACOS(config-service-matching-rules:a10.com)# hitcount-enable
ACOS(config-service-matching-rules:a10.com)# rule 1
ACOS(config-service-matching-rules:a10.co...)# domain-name equals
www.example.com
ACOS(config-service-matching-rules:a10.co...)# source-addr 10.214.6.0/24
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site k-
dc1 AllUp-or-PartUp
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-service-
ip a10-rs1 Up
ACOS(config-service-matching-rules:a10.co...)# health-state slb-server k-
dc1-link-1b Up
ACOS(config-service-matching-rules:a10.co...)# service www-view-cl1
ACOS(config-service-matching-rules:a10.co...)# exit
ACOS(config-service-matching-rules:a10.com)# rule 2
ACOS(config-service-matching-rules:a10.co...)# domain-name equals
www.example.com
ACOS(config-service-matching-rules:a10.co...)# source-addr 10.214.6.0/24
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site k-
dc1 Down
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site k-
dc2 AllUp-or-PartUp
ACOS(config-service-matching-rules:a10.co...)# health-state slb-server k-
dc1-link-1b Down
```

```
ACOS(config-service-matching-rules:a10.co...)# service www-view-cl2
```

gslb site

Description Configures a GSLB site.

Syntax

```
[no] gslb site site-name
```

Replace *site-name* with the name for the site (1-63 characters).

This command changes the CLI to the configuration level for the specified site, where the following site-related commands are available:

Command	Description
[no] active-rdt *option*	Configures options for the aRDT metric: • **aging-time** *minutes* –Specifies the maximum amount of time a stored aRDT result can be used. You can specify 1-15360 minutes. The default is 10 minutes. (“No” form of command is not available). • **bind-geoloc** – Stores the aRDT measurements on a per geo-location basis. Without this option, the measurements are stored on a per site-SLB device basis. • **ignore-count** *num* – Specifies the ignore count if aRDT is out of range. You can specify 1-15. The default is 5. • **limit** *num* – Specifies the maximum aRDT allowed for the site. If the aRDT measurement for a site exceeds the configured limit, GSLB does not eliminate the site. Instead, GSLB moves to the next metric in the policy. You can specify 1-16383 milliseconds (ms). The default is 16383. (“No” form of command is not available). • **mask** {/*mask-length* | *mask-ipaddr*} – Specifies

Command	Description
	the IPv4 client subnet mask length. The default mask length is 32. (“No” form of command is not available). • **ipv6-mask** {*/mask-length* | *mask-ipaddr*} – Specifies the IPv6 client subnet mask length. The default mask length is 64. (“No” form of command is not available). • **range-factor** *num* – Specifies the maximum percentage a new aRDT measurement can differ from the previous measurement. If the new measurement differs from the previous measurement by more than the allowed percentage, the new measurement is discarded and the previous measurement is used again. For example, if the range-factor is set to 25 (the default), a new measurement that has a value from 75% to 125% of the previous value can be used. Measurements is less than 75% or more than 125% of the previous measurement can not be used. You can specify 0-1000. The default is 25. • **smooth-factor** *num* – Blends the new measurement with the previous one, to smoothen the measurements. For example, if the smooth-factor is set to 10 (the default), 10% of the new measurement is used, along with 90% of the previous measurement. Similarly, if the smooth-factor is set to 50, 50% of the new measurement is used, along with 50% of the previous measurement. You can specify 1-100. The default is 10. (“No” form of command is not available).

Command	Description
	For more information, seeactive-rdt.)
[no] auto-map	Enables DNS auto-mapping for site resources.
[no] bw-cost *options*	Configures options for the BW-Cost metric: • **limit** *num*– Specifies the maximum amount the SNMP object queried by the GSLB ACOS Device can increase since the previous query, in order for the site to remain eligible for selection. You can specify 0-2147483647. There is no default. If a site becomes ineligible due to being over the limit, the *percentage* parameter is used. In order to become eligible for selection again, the site's limit value must not exceed *limit*threshold-percentage*. • **threshold** *percentage* – For a site to regain eligibility when BW-Cost is being compared, the SNMP object's value must be below the threshold-percentage of the limit value. You can specify 0-100. There is no default. For example, if the limit value is 80,000 and the threshold is 90 percent, then the limit value must be 72,000 or less, in order for the site to become eligible again based. Once a site again becomes eligible, the SNMP object's value is again allowed to increase up to the bandwidth limit (80,000 in this example). For more information, see bw-cost.
[no] controller *domain-name*	This command binds the specified controller to the configuration mode GSLB site in support of GSLB controller-based metrics. • *domain-name* – ACOS hostname of local controller

Command	Description
	for the GSLB site. There is no default.
[**no**] **disable**	Disables all servers in the GSLB site.
[**no**] **geo-location** *location-name*	Associates this site with a specific geographic location. (To configure a location, use the **gslb geo-location** command.)
[**no**] **ip-server** *service-ip*	Associates a real server with this site. • *service-ip* –Specify the real server name. Generally, virtual servers rather than real servers are associated with a site. To associate a virtual server with a site, use **vip-server** option of the **slb-dev** command.
[**no**] **slb-dev** *device-name* [*ip-addr*]	Specifies the device that provides SLB for the site. The IP address must be reachable by the GSLB controller when GSLB protocol is enabled. This command changes the CLI to the slb-dev configuration level where the following commands are available: • **admin-preference** *num* – Assigns a preference value to the SLB device. If the Admin-Preference metric is enabled in the policy and all metrics before this one result in a tie, the SLB device with the highest Admin-Preference value is preferred. You can specify from 0 – 255. The default is 100. • **auto-detect** {**ip** | **port** | **ip-and-port** | **disabled**} – Enables DNS auto detect at service IP level, port level, or both. You can also disable auto-detect. • **[no] auto-map** – Enables DNS auto-mapping for this site.

Command	Description
	• [no] **gateway** *ipaddr* – Specifies the gateway the SLB device will use to reach the GSLB local DNS for collecting aRDT measurements. • **gateway health-check** – Enables gateway health checking. A gateway health check is a Layer 3 health check (ping) sent to the gateway router for an SLB site. This option is enabled by default. • **gateway health-check-disable** – Disables gateway health checking. Gateway health check is enabled by default. • **IP Address** – Specifies the IPv4 address of the SLB device. • **IPv6 Address** – Specifies the IPv6 address of the SLB device. • **max-client** *num* – Specifies the maximum number of clients for which the GSLB ACOS Device (controller) saves data such as aRDT measurements for each of the clients. You can specify 1-2147483647. The default is 32768. • **NAME** – Host name of the SLB device. • [no] **proto-aging-fast** – This option enables a quick refreshowof data sent from a site ACOS Device to the ACOS controller by “aging out” data from a site ACOS Device. This can be used to obtain fresh health status information from a site ACOS. For example, when a virtual server is deleted from a site-ACOS Device, but this information could not be sent to the ACOS controller, then the status in the controller will continue to appear as "UP" for a long time until it is aged out. The "proto-aging-fast" command forces the GSLB controller to start aging the health status immediately after receiving

Command	Description
	updated information from a site ACOS. • **proto-aging-time** *seconds* – If communication between a site ACOS Device and the GSLB controller is interrupted, then the data for that site will become stale. The GSLB controller can continue to rely upon this old information, but after some time, the old data for the site must be purged. The lifespan of this old data is the sum of the time set using the gslb protocol status-interval command, plus the time you set using this proto-aging-time option. The default value is 60 seconds. You can specify from 1 to 65535 seconds. • [**no**] **proto-compatible** – Enables GSLB protocol compatibility between a controller running 2.6.1 or later and a site ACOS Device running 2.4.x. This option is disabled by default. • **resolve-to-ipv4** – Use A query only to resolve FQDN. It is the default query type. • **resolve-to-ipv6** – Use AAAA query only to resolve FQDN. • **resolve-to-ipv4-and-ipv6** – Use A and AAAA query only to resolve FQDN. • [**no**] **vip-server** {*name* | *ipaddr*} – Maps this SLB site to a globally configured GSLB service IP address. If you use the *name* option, the name must be the name of a configured service IP. (To configure the service IP, use the gslb service-ip. **NOTE:** The same vip-server can be added under multiple slb-devices within a site.

Command	Description
	NOTE: For the FQDN slb-device, the vip-servers bound on the host name slb-device are inherited by the first dynamic slb-device resolved from the dns query. • **gslb site document slb-dev document 8.8.8.8 msg-format-acos-2x** This option sets up compatibility of GSLB Protocol Health Check between ACOS version 2.x and 4.1.4-GR1.
[**no**] **template** *template-name*	Binds a template to the site. To use the BW-Cost metric, use this option to bind a GSLB SNMP template to the site.
[**no**] **weight** *num*	Assigns a weight to the site. If the Weighted-Site metric is enabled in the policy and all metrics before Weighted-Site result in a tie, the site with the highest weight is preferred. The weight can be from 1 – 100. The default is 1.

Default See descriptions.

Mode Global configuration mode

Example The following example creates a site named “NY-site” and adds SLB ACOS Device “site-acos-1” with IP address 10.10.10.10 to the site:

```
ACOS(config)# gslb site NY-site
ACOS(config-gslb site:NY-site)# slb-dev site-acos-1
10.10.10.10
ACOS(config-gslb site:NY-site-slb dev:sit...)#
```

gslb sync-objects

Description Configures objects as additional targets for GSLB synchronization in an L3V partition. During GSLB synchronization, the GSLB master node

synchronizes its configuration for the specified objects with the controller nodes in the GSLB group.

Syntax

```
[no] gslb sync-objects [object class | action {enable | disable} ]
```

Parameter	Description
object class	Specifies the object to be synchronized from the master node to members in a GSLB group as a part of GSLB synchronization. The synchronization only considers common ACOS objects, such as, slb.server, slb.service-group, slb.virtual-server, health.monitor, and so on.
action	Enable or disable the action for synchronizing the specified object.

Default Disabled

Mode Global configuration mode

Usage This command enables the synchronization of additional required ACOS objects, such as, real servers, service-groups, or virtual servers, from the GSLB master to all other members in the GSLB Controller group. For this, all the member nodes in the GSLB group must run the same software release version.

The **gslb sync-objects** should use appropriate tagging. For example, `gslb sync-objects slb.server` and `gslb sync-objects slb` cannot be used simultaneously.

Example This example configures GSLB synchronization objects for SLB real server and health monitor configurations. The SLB real server and health monitor configurations will get synchronized to the GSLB members from the GSLB master. The **gslb sync-objects action enable** command enables the GSLB synchronization when the member connects to the master node.

```
ACOS(config)# gslb sync-objects slb.server
ACOS(config)# gslb sync-objects health.monitor
ACOS(config)# gslb sync-objects action enable
```

gslb system age-interval

Description Set the age interval for runtime GSLB statistics.

Syntax

```
gslb system age-interval seconds
no gslb system age-interval
```

Replace *seconds* with the desired age interval (0-120 seconds).

Default 10 seconds

Mode Global configuration mode

gslb system auto-map module

Description Enable auto-mapping of IP address to resource name.

Syntax

```
gslb system auto-map module resource-type
no gslb system auto-map module
```

Parameter	Description
resource-type	Enables DNS auto-mapping for the specified resource type. When auto-mapping is enabled, ACOS can respond to DNS queries for resources of the specified type that are within the GSLB zone. The *resource-type* option can be one of the following: • **gslb-group** – Enables auto-mapping for GSLB groups. • **gslb-service-ip** – Enables auto-mapping for service-IPs. • **gslb-site** – Enables auto-mapping for GSLB sites. • **hostname** – Enables auto-mapping for the ACOS Device hostname. • **slb-device** – Enables auto-mapping for SLB devices. • **slb-server** – Enables auto-mapping for real server names.

Parameter	Description
	• **slb-virtual-server** – Enables auto-mapping for virtual server names.

Default Disabled

Mode Global configuration mode

gslb system auto-map ttl

Description Configure the TTL for DNS A or AAAA records created by the auto-mapping feature.

Syntax

```
gslb system auto-map ttl seconds
no gslb system auto-map ttl
```

Replace seconds with the maximum number of seconds for which an A or AAAA record created by auto-mapping is valid. You can specify 1-65535 seconds.

Default 300 seconds

Mode Global configuration mode

gslb system geo-location load

Description Load a geo-location database into GSLB. Using a geo-location database is an alternative to manually configuring each geo-location separately.

Syntax

```
[no] gslb system geo-location load
{iana | file-name csv-template-name}
```

Parameter	Description
iana	Loads the Internet Assigned Numbers Authority (IANA) database. The IANA database contains the geographic locations of the IP address ranges and subnets assigned by the IANA. The IANA database is included in the ACOS system software. The IANA geo-

Parameter	Description
	location database is loaded by default.
file-name csv-template-name	Loads a custom database. You can load a custom geo-location database from a file in comma-separated-values (CSV) format. This option requires configuration of a CSV template on the ACOS Device. When you load the CSV file, the data is formatted based on the template. To configure a CSV template, see gslb template csv.

Mode Global configuration mode

Usage You can load more than one database. The **geo-location match** command determines the IP address used when databases contain overlapping addresses.

Example The following command loads the IANA database:

```
ACOS(config)# gslb system geo-location load iana
```

Example The following command loads geo-location data from a CSV file:

```
ACOS(config)# gslb system geo-location load test1.csv test1-template
```

gslb system ip-ttl

Description Change the IP Time-to-Live (TTL) in DNS replies to clients.

Syntax

```
gslb system ip-ttl num
no gslb system ip-ttl
```

Replace *num* with the desired TTL value (0-255).

Default 0

Mode Global configuration mode

Usage This option applies only to DNS server mode. The option does not apply to DNS proxy mode.

The TTL value is used in all replies, regardless of the client's original TTL.

gslb system wait

Description Delay startup of GSLB following startup of the ACOS Device.

Syntax

```
gslb system wait seconds
no gslb system wait
```

Replace *seconds* with the desired startup delay interval (0-16384 seconds).

Default 0 seconds (no delay)

Mode Global configuration mode

gslb template csv

Description Configure a template for extracting geo-location data from an imported CSV file.

Syntax

```
[no] gslb template csv template-name
```

Replace *template-name* with the name of the template (1-63 characters).

This command changes the CLI to the configuration level for the specified template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See the *CLI Reference*.)

Parameter	Description
[no] delimiter {*character* | *ASCII-code*}	Specifies the character used in the file to delimit fields. You can type the character or enter its decimal ASCII code (0-255).
[no] field *num type-of-data*	The *num* option specifies the field position within the CSV file. You can specify from 1-64. The following options specify the type of geo-location that is

Parameter	Description
	located in the field position: • **ip-from** – Specifies beginning IP address in range or subnet. • **ip-to-mask** – Specifies ending IP address in range or subnet mask. • **continent** – Specifies continent location of IP address range or subnet. • **country** – Specifies country location of IP address range or subnet. • **state** – Specifies state location of IP address range or subnet. • **city** – Specifies city location of IP address range or subnet.
[no] ipv6-enable	Support IPv6 IP ranges.

Default There is no default CSV template. When you configure one, the field locations are not set. The default delimiter character is a comma (,).

Mode Global configuration mode

Usage To load a geo-location data file and use the CSV template to extract the data, see gslb system geo-location load.

Example The following commands configure a CSV template called “test1-tmplte”:

```
ACOS(config)# gslb template csv test1-tmplte
ACOS(config-csv:test1-tmplte)# field 1 ip-from
ACOS(config-csv:test1-tmplte)# field 2 ip-to-mask
ACOS(config-csv:test1-tmplte)# field 5 continent
ACOS(config-csv:test1-tmplte)# field 3 country
```

gslb template snmp

Description Configure an SNMP template to query data for use by the BW-Cost metric.

Syntax

```
[no] gslb template snmp template-name
```

Replace *template-name* with the name of the template (1-63 characters).

This command changes the CLI to the configuration level for the specified template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See the *CLI Reference*.)

Parameter	Description
[no] auth-key *string*	Specifies the authentication key. The key *string* can be 1-127 characters long. This command is applicable if the security level is **auth-no-priv** or **auth-priv**.
[no] auth-proto {**sha** | **md5**}	Specifies the authentication protocol. This command is applicable if the security level is **auth-no-priv** or **auth-priv**.
[no] community *community-string*	For SNMPv1 or v2c, specifies the community string required for authentication.
[no] context-engine-id *id*	Specifies the ID of the SNMPv3 protocol engine running on the site ACOS Device.
[no] context-name *id*	Specifies an SNMPv3 collection of management information objects accessible by an SNMP entity.
[no] host {*name* | *ipaddr*}	Specifies the IP address of the site ACOS Device.

Parameter	Description
[**no**] **interface** *id*	Specifies the SNMP interface ID. 0-2147483647
[**no**] **interval** *seconds*	Specifies the amount of time between each SNMP GET to the site ACOS Devices. You can specify 1-999 seconds. The default is 3.
[**no**] **oid** *oid-value*	Specifies the interface MIB object to query on the site ACOS Device. If the object is part of a table, make sure to append the table index to the end of the OID. Otherwise, the ACOS Device will return an error.
[**no**] **port** *portnum*	Specifies the protocol port on which the site ACOS Devices listen for the SNMP requests from the GSLB ACOS Device. You can specify 1-65535. The default is 161.
[**no**] **priv-key** *string*	Specifies the encryption key. The key *string* can be 1-127 characters long. This command is applicable only if the security level is **auth-priv**.
[**no**] **priv-proto** {**aes** | **des**}	Specifies the privacy protocol used for encryption. This command is applicable only if the security level is **auth-priv**.
[**no**] **security-engine-id** *id*	Specifies the ID of the SNMPv3 security engine running on the site ACOS Device. For each command, the ID is a string 1-127 characters long.
[**no**] **security-level** {**no-auth** | **auth-no-priv** | **auth-priv**}	Specifies the SNMPv3 security level: • **no-auth** – Authentication is not used and encryption (privacy) is not used. This is the default. • **auth-no-priv** – Authentication is used but encryption is not used. • **auth-priv** – Both authentication and encryption are used.

Parameter	Description
[**no**] **username** *name*	Specifies the SNMPv3 username required for access to the SNMP agent on the site ACOS Device.
[**no**] **version** {**v1** | **v2c** | **v3**}	Specifies the SNMP version running on the site ACOS Device.

Default See above.

Mode Global configuration mode

Usage The **community** command applies only to SNMPv1 or v2c. Most of the other commands, with the exception of the **version**, **interval**, **port**, and **interface** commands, apply to SNMPv3.

You can not delete an SNMP template if the template is in use by a site. To delete a template, first remove it from all site configurations that are using it.

Example The following commands configure a GSLB SNMP template for SNMPv2c:

```
ACOS(config)# gslb template snmp snmp-1
ACOS(config-snmp:snmp-1)# version v2c
ACOS(config-snmp:snmp-1)# host 192.168.214.124
ACOS(config-snmp:snmp-1)# oid .1.3.6.1.2.1.2.2.1.16.12
ACOS(config-snmp:snmp-1)# community public
ACOS(config-snmp:snmp-1)# exit
```

Example The following commands configure a GSLB SNMP template for SNMPv3. In this example, authentication and encryption are both used.

```
ACOS(config)# gslb template snmp snmp-2
ACOS(config-snmp:snmp-2)# security-level auth-priv
ACOS(config-snmp:snmp-2)# host 192.168.214.124
ACOS(config-snmp:snmp-2)# username read
ACOS(config-snmp:snmp-2)# oid .1.3.6.1.2.1.2.2.1.16.12
ACOS(config-snmp:snmp-2)# priv-proto des
ACOS(config-snmp:snmp-2)# auth-key 12345678
ACOS(config-snmp:snmp-2)# priv-key 12345678
```

gslb zone

Description Configures a GSLB zone, which identifies the top-level name for the services load balanced by GSLB.

Syntax

```
[no] gslb zone zone-name
```

Replace *zone-name* with the name of the zone, up to 127 alphanumeric characters, or * (wildcard character matching on all zone names).

You can use lower case characters and upper case characters. However, since Internet domain names are case-insensitive, the ACOS Device internally converts all upper case characters in GSLB zone names to lower case.

NOTE: DNSSEC is not supported for GSLB wildcard zones.

This command changes the CLI to the configuration level for the specified zone, where the following zone-related commands are available:

Command	Description
[no] **disable**	Disables all services in the GSLB zone.
[no]**dns-caa-record** [**Issuer Critical Flag**] [**Issue**] [**Issuewild**] [**Iodef**] [**NAME**] [**Rdata**] [**ttl** *seconds*]	Configures a DNS Certification Authority Authorization (CAA) record for the GSLB zone. • **Issuer Critical Flag** - It is an octet. The default value is 0. The customer can define the other values up to 255 characters. • **Issue** - Instructs the certificate authorities (CA) to issue the certificate only for the specified domain. It is a sequence of characters including only 'a' to 'z', 'A' to 'Z', '0' to '9'. I can be up to 1000 characters. • **Issuewild** - Allows the CA to issue the wild card certificate that can be used in a domain or sub-

Command	Description
	domain. It can be up to 1000 characters. • **Iodef** - Specified an url. It allows the CA to send violation report to the specified email or contact details. It can be up to 1000 characters. • **NAME** - Specifies other property tags. It can be up to 255 lowercase alphanumeric characters. • **Rdata** - Specifies only the domain name or domain name along with other parameters or only URL behind iodef. It can be up to 1000 characters. • **ttl** - Specifies the number of seconds GSLB will cache and reuse negative replies (NXDOMAIN messages). A negative reply is an error message indicating that a requested domain does not exist. **NOTE:** The **ttl** option is equivalent to the "minimum" option in BIND 9.
[**no**]**dns-mx-record** *name priority* [**ttl** *num*]	Configures a DNS Mail Exchange (MX) record for the zone. The *name* is the fully-qualified domain name of the mail server for the zone. If more than one MX record is configured for the same zone, the *priority* specifies the order in which the mail server should attempt to deliver mail to the MX hosts. The MX with the lowest priority value has the highest priority and is tried first. The *priority* can be 0-65535. There is no default. MX records configured on a zone are used only for services on which MX records are not configured.

Command	Description
	NOTE: • If you want the GSLB ACOS Device to return the IP address of the mail service in response to MX requests, you must configure Address records for the mail service. • Optionally, you can configure the Time-to-Live in seconds. The range is from 0-2147483647 seconds.
[no] dns-ns-record *domain-name* [**ttl** *num*]	Configures a DNS name server record for the specified domain. Optionally, you can configure the Time-to-Live in seconds. The range is from 0-2147483647 seconds.
[**no**] **dns-soa-record** [**external**] *dns-server-name mailbox-name* [**expire** *seconds*] [**refresh** *seconds*] [**retry** *seconds*] [**serial** *num*] [**ttl** *seconds*]	Configures a DNS start of authority (SOA) record for the GSLB zone. • **external** - causes the ACOS Device to replace the internal SOA record with an external SOA record when a request is received from an external client. This prevents external clients from gaining access to internal information. The feature must also be enabled in the GSLB policy. • **refresh** - specifies the number of seconds other DNS servers wait before requesting updated information for the GSLB zone. The **retry** option specifies how many seconds other DNS servers wait before resending a refresh request, if GSLB does not respond to the previous request. The **expire** option specifies how many seconds GSLB can remain unresponsive to a refresh request before the other DNS server drops responding to queries for the zone.

Command	Description
	• **serial** - specifies the initial serial number of the SOA record. This number is automatically incremented each time a change occurs to any records in the zone file. You can specify a serial number from 0-2147483647. The default is based on the current system time on the GSLB ACOS Device when you create the SOA record. • **ttl** - specifies the number of seconds GSLB will cache and reuse negative replies (NXDOMAIN messages). A negative reply is an error message indicating that a requested domain does not exist. **NOTE:** The **ttl** option is equivalent to the "minimum" option in BIND 9.
[**no**] **policy** *policy-name*	Applies the specified GSLB policy to the zone. You can specify "default" for the GSLB policy name, if you have not configured another policy and applied it to the zone. The GSLB policy applied to the zone is also applied to the services in that zone.
[**no**] **service** *port* [*service-name*]	Adds a service to the zone. The *port* option specifies the service port and can be a port number from 0 to 65534. The *service-name* can be 1-63 alphanumeric characters. For the same reason described for zone names, the ACOS Device converts all upper case characters in GSLB service names to lower case. This command changes the CLI to the configuration level for the service, where the following GSLB-related commands are available: • **action** *action-type* – Specifies the action to perform for DNS traffic: ◦ **drop** – Drops DNS queries from the local DNS

Command	Description
	server. ◦ **forward { both** | **query** | **response}** – Forwards requests or queries, as follows: ◦ **forward both** – Forwards queries to the Authoritative DNS server, and forwards responses to the local DNS server. ◦ **forward query** – Forwards queries to the Authoritative DNS server, but does not forward responses to the local DNS server. ◦ **forward response** – Forwards responses to the local DNS server, but does not forward queries to the Authoritative DNS server. ◦ **ignore** – Ignores the request. ◦ **reject** – Rejects DNS queries from the local DNS server and returns the "Refused" message in replies. **NOTE:** Use gslb dns action must be enabled in the GSLB policy.
[**no**] **service** *port* [*service-name*] (cont.)	GSLB-related commands are available: • **disable** – Disables all services in the GSLB zone. • **dns-a-record** [**ip** *service-ipaddr* | ***service-name*** {**as-backup** | **as-replace** | **no-resp** | **static** | **ttl** *num* | **weight** *num*}] – Configures a DNS Address (A) record for the service, for use with the dns ip-replace option in the GSLB policy. The *service-name* can contain 1-63 alphanumeric characters or * (wildcard character matching on all service names). ◦ **as-backup** – This option is used to specify the

Command	Description
	backup servers in the dns-a-record within the GSLB zone. These are the servers that will be returned to the client if the primary servers fail and backup server mode is enabled. ◦ **as-replace** – This option is used with the **ip-replace** option in the policy. When both options are set (**as-replace** here and **ip-replace** in the policy), the client receives only the IP address set here by **service-ip**. ◦ **disable**– Disables DNS records for this service in the zone. ◦ **no-resp**– Prevents the IP address for this site from being included in DNS replies to clients. ◦ **static**– This option is used with the **dns server** option in the policy. When both options are set (**static** here and **dns server** in the policy), the GSLB ACOS Device acts as the DNS server for the IP address set here by **service-ip**. ◦ **ttl** *num*– Assigns a TTL to the service, 0-2147483647. By default, the TTL of the zone is used. This option can be used with the **dns server** option in the policy, or with DNS proxy mode enabled in the policy. ◦ **weight** *num*– Assigns a weight to the service. If the Weighted-IP metric is enabled in the policy and all metrics before Weighted-IP result in a tie, the service on the site with the highest weight is selected. The weight can be 1-100. By default, the weight is not set. ◦ **server-name**– Contains the list of configured real servers and GSLB service IPs.

Command	Description
	NOTE: The **no-resp** option is not valid with the **static** or **as-replace** option. If you use **no-resp**, you cannot use **static** or **as-replace**. **NOTE:** The **dns-a-record {service-name |ip}** command supports the addition of only 256 records.
[**no**] **service** *port* [*service-name*] (cont.)	• **dns-cname-record** *alias* [*alias ...*] [**as-backup**] [**admin-preference** *num*] [**weight** *num*] – Configures DNS Canonical Name (CNAME) records for the service. • **admin-preference** *num*– Specify the administrative preference. If using the Alias Admin Preference metric, then the DNS CNAME record with the highest administratively set preference is selected. Default is 100. • **as-backup** – Specifies that the record is a backup record. • **sampling-enable** – Specifies if baselining should be enabled. ◦ **all** - enables sampling of all CNAME records. ◦ **cname-hits** - Specifies the number of times the CNAME has been used. • **weight** *num* – Specify the weight. If using the Weighted Alias metric, then the DNS CNAME record with the highest weight is selected. Default is 1. • **dns-mx-record name** *priority* [**ttl***num*] – Configures a DNS Mail Exchange (MX) record for the service. The *name* is the fully-qualified domain

Command	Description
	name of the mail server for the service. If more than MX record is configured for the same service, the *priority* specifies the order in which the mail server should attempt to deliver mail to the MX hosts. The MX record with the lowest priority number has the highest priority and is tried first. The *priority* can be 0-65535. There is no default. **NOTE:** If you want the GSLB ACOS Device to return the IP address of the mail service in response to MX requests, you must configure A records for the mail service. • **dns-naptr-record** *name* **service-proto** *name {flagname | order num preference num {regexp | ttl}}*– Configures a Name Authority Pointer (NAPTR) record for the service. It can contain a replacement or regular expression. ◦ **service-proto** - Specifies the service and protocol to be used. The name can be 1-127 characters long. ◦ **flag name** Within this, you can specify the flag, such as, a or s. The default value is empty. ◦ **order**, specify the order and **preference** (0-65535). ◦ **regexp** is used to return regular expression. ◦ **ttl** specifies the time-to-live for the DNS record in seconds. Typically DNS records take 24-48 hours to propagate. • **dns-ns-record** *domain-name* **as-backup**][**ttl** *num*] – Configures a DNS name server record. To

Command	Description
	use the **as-backup** option, you also must use the dns backup-alias command in the policy. • **dns-ptr-record** *domain-name* [**ttl** *num*] – Configures a DNS pointer record. • **dns-srv-record** *domain-name* **port** *portnum priority* [weight *num*] [**ttl** *num*] – Configures a DNS service record. ◦ The **port** *portnum* specifies the protocol port to return to the client, and can be 0-65534. There is no default. You must specify a port. ◦ The *priority* can be 0-65535. There is no default. ◦ The **weight** *num* specifies the weight and can be 0-65535. The default is 10. ◦ The **ttl** specifies the time-to-live for the DNS record in second. Typically DNS records take 24-48 hours to propagate.
[**no**] **service** *port* [*service-name*] (cont).	• **dns-txt-record** *obj-name txt-data* [**ttl** *num*] – Enables use of DNS TXT resource records to carry multiple pieces of DNS TXT data within one TXT record. ◦ The *obj-name* specifies the text data's object name, in order to avoid long URLs of aXPAPI. ◦ The *txt-data* is the DNS TXXT data that you want inputted in the TXT record. ◦ The **ttl** specifies the time-to-live for the DNS record in second. Typically DNS records take 24-48 hours to propagate.

Command	Description
	NOTE: The ACOS Device has a special handler that enables you to enter non-printable characters that the CLI does not support. **NOTE:** This option also requires the **dns server txt** command at the configuration level for the GSLB policy. • **geo-location** *location-name* - Configures geo-location settings. The location must already be configured. (See gslb geo-location.) Entering this command takes you to the GSLB Zone Service Geo-location configuration level, where the following commands are available: • **action** *action* – Specifies the action to perform for DNS traffic. The *action* options are the same as those for the **action** command described above. Another action possible is **allow**, which allows queries from this geo-location. • **alias** *url* – Maps an alias configured with the **alias** option (see above) to the specified location for this service. • **policy** *policy-name* – Applies the specified GSLB to clients from the geo-location. • **health-check-gateway enable** – Enable service's health-check gateway. • **health-check-gateway disable** – Disable service's health-check gateway. • **health-check-port** *portnum* – Specify the port for the health check for the service. Use multiple statements to configure more than one port. • **policy** *policy-name* — Applies the specified GSLB

Command	Description
	policy to the service. If the service policy is the default policy, then the service will automatically inherit the policy configured for the overall GSLB Zone. Any non-default policy configured for the service specifically will be honored over the GSLB Zone policy.
[**no**] **service** *port* [*service-name*] (cont).	• **dns-caa-record** *Issuer Critical Flag Issue Issuewild Iodef Name* [**ttl** *num*] - Configures caa records for the service. The **ttl** specifies the time-to-live for the DNS record in second. Typically DNS records take 24-48 hours to propagate. • **Issuer Critical Flag** - It is an octet. The default value is 0. The customer can define the other values up to 255 characters. • **Issue** - Instructs the certificate authorities (CA) to issue the certificate only for the specified domain. It is a sequence of characters including only 'a' to 'z', 'A' to 'Z', '0' to '9'. It can be up to 1000 characters. • **Issuewild** - Allows the CA to issue the wild card certificate that can be used in a domain or sub-domain. It can be up to 1000 characters. • **Iodef** - Specifies an url. It allows the CA to send violation report to the specified email or contact details. It can be up to 1000 characters. • **NAME** - Specifies other property tags. It can be up to 255 lowercase alphanumeric characters. • **Rdata** - Specifies only the domain name or domain name along with other parameters or only URL behind iodef. It can be up to 1000 characters.

Command	Description
[no] **template dnssec** *template-name*	Binds a DNSSEC template to the zone.
[no] **ttl** *seconds*	Changes the TTL of each DNS record contained in DNS replies received from the DNS for which the ACOS Series is a proxy, for this zone. You can specify from 0 to 1000000000 (one billion) seconds. This TTL setting overrides the TTL setting in the GSLB policy. The default is 10. The TTL of the DNS reply can be overridden in two different places in the GSLB configuration: (1) If a GSLB policy is assigned to the individual service, then the TTL from that policy is used. (2) If no policy is assigned to the individual service, but the TTL is set in the zone, then the zone's TTL setting is used. (This is the level set by the **ttl** command shown earlier this section.)
[no] **use-server-ttl**	Use the configured service Time-to-Live.

Default Default settings are described above, where applicable.

Mode Global configuration mode

Example The following example creates a zone named "acos-gslb-zone":

```
ACOS(config)# gslb zone acos-gslb-zone
ACOS(config-zone:acos-gslb-zone)#
```

Example The following example uses the wildcard character at the end of the **gslb zone** command. This has the result of identifying all GSLB zones so that the next line of the configuration creates a positive match on all DNS domains that have the prefix of "www".

```
ACOS(config)# gslb zone *
ACOS(config-zone *)# service 80 www
```

Example The following commands create a default GSLB policy and then specify that a backup server at IP 10.10.2.1 will be returned to the client if the primary servers fail.

```
ACOS(config)# gslb policy default
ACOS(config-policy:default)# dns backup-server
ACOS(config-policy:default)# exit
ACOS(config)# gslb zone z1
ACOS(config-zone:z1)# service 80 http
ACOS(config-zone:z1-service:http)# dns-a-record 10.10.2.1 as-
backup
ACOS(config-zone:z1-service:http)# exit
ACOS(config-zone:z1)# exit
ACOS(config)#
```

Example The following commands create the failover gslb policy in the z1 zone. Configure dns-a-record for the real server and service with a matching label. Here, **http** and **gitlab**. The service port number should match the real port number. Custom health checks can be bound to each real port.

```
ACOS(config)(NOLICENSE)#gslb zone z1
ACOS(config-zone:z1)(NOLICENSE)#policy failover
ACOS(config-zone:z1)(NOLICENSE)#service 80 http
ACOS(config-zone:z1-service:http)(NOLICENSE)#dns-a-record slb1
http static
ACOS(config-zone:z1-service:http)(NOLICENSE)#dns-a-record slb2
http static
ACOS(config-zone:z1)(NOLICENSE)#service 80 gitlab
ACOS(config-zone:z1-service:gitlab)(NOLICENSE)#dns-a-record
slb1 gitlab static
ACOS(config-zone:z1-service:gitlab)(NOLICENSE)#dns-a-record
slb2 gitlab static
```

import geo-location

Description Imports new geo-location database CSV files into an ACOS Device.

Syntax

```
import geo-location file-name [overwrite] [use-mgmt-port] url
period  num]
```

The **overwrite** option overwrite the existing geo-location file under that name with the new geo-location file that is being imported.

Default If no database is loaded, the default is a pre-loaded IANA database.

Mode Global configuration mode.

Usage This command imports a geo-location database, saved as a CSV file, into an ACOS Device and allows for periodic synchronization of the database across all GSLB group members. This command only imports a database; it does not load the database into the ACOS starting configuration. To load the database file, see gslb system geo-location load.

Example The following command imports a geo-location database CSV file and configures ACOS to periodically check for updates once a day:

```
ACOS(config)# import geo-location test1.csv
ftp://192.168.1.100
User name []?admin2
Password []?*********
File name [/]?test1.csv
```

ip dns

Description Enable the command at DNS primary, secondary server, or for particular DNS in the L3V partition support

Syntax

```
ip dns {primary | secondary | suffix {ipv4_address | ipv6_
address | <dns_name>}
```

Parameter	Description
primary	Primary DNS server.
secondary	Secondary DNS server.
suffix	DNS suffix
ipv4_address	IPv4 address of DNS server.
ipv6_address	IPv6 address of DNS server.
<name>	DNS suffix name, valid range length of string 1 to

Parameter	Description
	32 characters.

Default NA

Mode Configuration mode L3V partition

Example

```
ACOS[L3v-partition-name](config)# ip dns
```

Show Commands

show counters gslb dns

Description Displays GSLB metric selection global counters.

Syntax

```
show counters gslb dns
```

Default NA

Mode All

Usage Configure ACOS with GSLB configuration in shared and L3v partitions.

Example Example output on GSLB master or controller device.

```
ACOS-Active-vMaster[11/1]-gslb:Master# show counters gslb dns

Total number of DNS queries received                2733965689
Total number of DNS replies sent to clients         1697727
Number of queries with incorrect data length        180
Number of replies with incorrect data length        0
Number of queries with incorrect header             1760911
Number of replies with incorrect header             1063966
Number of queries with incorrect format             94462
Number of replies with incorrect format             30410
Number of queries with unknown service              779786676
Number of replies with unknown service              39375
```

```
Number of queries with incorrect class              151
Number of replies with incorrect class              216
Number of queries with incorrect type               348
Number of replies with incorrect type               389
Number of replies with unknown server IP            6466
Metric Health Check Hit                             1949111169
Metric Weighted IP Hit                              389739775
Metric Weighted Site Hit                            389739867
Metric Capacity Hit                                 782531473
Metric Active Server Hit                            392791697
Metric Easy RDT Hit                                 0
Metric Active RDT Hit                               389739813
Metric Geographic Hit                               389945758
Metric Connection Load Hit                          392791546
Metric Number of Sessions Hit                       392791547
Metric Active Weight Hit                            0
Metric Admin Preference Hit                         389739921
Metric Bandwidth Quality Hit                        0
Metric Bandwidth Cost Hit                           392791697
Metric User Hit                                     0
Metric Least Reponse Hit                            782531468
Metric Admin IP Hit                                 389739775
Metric Round Robin Hit                              205983
Metric Connection Count by Site Hit                 4
```

show domain-list

Description Shows the configuration log for the domain-list for FQDN, domain name, and the IP's that are associated to the list.

Syntax

```
show domain-list <list_name> [resolved | unresolved]
```

<list_name>	Domain list name of maximum length 63 characters.
	Resolved FQDN domain information.
	Unresolved domain information.

Mode Global configuration mode

Example

```
ACOS(config)# show domain-list FQDN_list1
        1 FQDN was resolved; 1 FQDN was not resolved
        Server1.com  hitcount 10311
            Number of IPv4 IPs:2
            10.1.1.2
            10.1.1.3
             Number of Ipv6 IPs:1
             2018:1::32
      Server2.com hitcount 0
          Number of Ipv4Ps:0
         Number of Ipv6 IPs:0

ACOS(config)# show domain-list FQDN_list1 resolved
   1 FQDN_list1 was resolved
    Server1.com          10311
            Number of IPv4 IPs:2
            10.1.1.2
            10.1.1.3
             Number of Ipv6 IPs:1
             2018:1::32

ACOS(config)# show domain-list FQDN_list1 unresolved
    1 FQDN was not resolved
        Server2.com hitcount 0
          Number of Ipv4Ps:0
         Number of Ipv6 IPs:0
```

show gslb cache

Description Show the DNS messages cached on the GSLB ACOS Device. The GSLB ACOS Device caches DNS replies if either of the following GSLB policy options are enabled:

- DNS caching
- aRDT metric (if the single-shot option is used)

Syntax

```
show gslb cache
[match domain-name]
[service-name ...]
[zone zone-name] ]
```

Parameter	Description
match *domain-name*	Displays cached DNS messages for the matched domain.
service-name	Displays cached DNS messages for the specified service.
zone *zone-name*	Displays cached DNS messages for the specified zone.

Mode All

Example The following command displays cached DNS messages for service “www.testme.com:http”.

```
ACOS# show gslb cache www.testme.com:http
              QD = Question Records,  AN = Answer Records
              NS = Authority Records, AR = Additional Records
              Flag = DNS Flag, Len = Cache Length
              A = Authoritative Answer, D = Recursion Desired
              R = Recursion Available
Zone: testme.com
Service              Alias       Len   TTL     Flag QD  AN  NS
AR
-------------------------------------------------------------------
----
www.testme.com:http              96    3055     DR   1   4   0
 0
```

The following table describes the fields in the command output.

Field	Description
Zone	GSLB zone name.
Service	GSLB service.
Alias	Alias, if configured, that maps to the DNS Canonical

Field	Description
	Name (CNAME) for the service.
Len	Length of the DNS message, in bytes.
TTL	Number of seconds for which the cached message is still valid.

show gslb config

Description Show the GSLB configuration commands that are in the running-config.

Syntax

```
show gslb config
[
active-rdt |
dns |
geo-location |
group |
ip-list |
policy |
protocol |
service-group |
service-ip |
site |
system
template |
view |
zone
]
```

Mode All

Usage The “show gslb config” command can be used in shared partitions, L3V partitions, and GSLB view.

When used within a shared partition, the show gslb config command can include the following:

- active-rdt: Show GSLB aRDT configuration
- dns: Show GSLB global DNS configuration
- geo-location: Show GSLB global geo-location configuration
- group: Show GSLB group configuration
- ip-list: Show GSLB IP list configuration
- policy: Show GSLB policy configuration
- protocol: Show GSLB protocol configuration

- service-group: Show GSLB service-group configuration
- service-ip: Show GSLB service-ip configuration
- site: Show GSLB site configuration
- system: Show GSLB system options
- template: Show GSLB template configuration
- view: Show GSLB view
- zone: Show GSLB zone configuration
- error counter:

When used in L3V partitions

When used within a L3V partition, the **`show gslb config`** command can include the following:

- group: Show GSLB Group configuration
- ip-list: Show GSLB IP list configuration
- policy: Show GSLB policy configuration
- service-ip: Show GSLB service-IP configuration
- site: Show GSLB site configuration
- template: Show GSLB template configuration
- zone: Show GSLB zone configuration

NOTE: When the **`show gslb config`** command is used within a L3V partition, the following command completions are not supported: active-rdt, dns, geo-location, protocol, system, and view.

When used in gslb-view

When used in gslb-view, the **`show gslb config`** command can include the following:

- group: Show GSLB Group configuration
- ip-list: Show GSLB IP list configuration
- policy: Show GSLB policy configuration
- site: Show GSLB site configuration
- template: Show GSLB template configuration
- zone: Show GSLB zone configuration

NOTE: When the **show gslb config** command is used in gslb-view, the following command completions are not supported: active-rdt, dns, geo-location, protocol, service-ip, system, and view.

Details about L3V Deployments

When using the new **show gslb config** command filters in L3V partitions, only the following command completions are supported: group, ip-list, policy, service-ip, site, template, and zone.

The following **show gslb config** command options are not supported in L3V deployments, and by extension, not supported by the new gslb show command enhancements: active-rdt, dns, geo-location, protocol, system and view.

CLI Example

- Show gslb config zone
- Show gslb config site zone
- Show gslb config service-ip zone | include aaa

Show gslb config for gslb-view

The command syntax when used within gslb-view is as follows:

```
show gslb config
[
group |
ip-list |
policy |
service-ip |
site |
template |
zone |
common filters(| include xxx)
]
```

show gslb fqdn

Description Shows GSLB statistics using a Fully Qualified Domain Name (FQDN).

Syntax

```
show gslb fqdn  domain-name [domain-name ... ]
[
cache |
dns-a-record |
dns-caa-record |
dns-cname-record |
dns-mx-record |
dns-ns-record |
dns-ptr-record |
dns-srv-record |
dns-txt-record |
session
]
```

Mode All

show gslb geo-location

Description Show the status of GSLB geo-location mappings.

Syntax

```
show gslb geo-location
{
[db [geo-location-name]
    [[statistics] ip-range  range-start range-end]
    [[statistics] depth  num]
    [[statistics] directory  num]
    [[statistics] top  num [percent [global]]]
    [statistics]]

[file [file-name]]

[ip  ipaddr [statistics] [policy  policy-name]]

[ipv6  ipv6addr [statistics] [policy  policy-name]]

[rdt
  [active [geo-location-name ...]
          [site site-name] [depth num]]
```

Parameter	Description
db *[options]*	Displays the geo-location database. If you specify a geo-location name, only the entries for that geo-location are shown. Otherwise, entries for all geo-locations are shown. • **ip-range** – Displays entries for the specified IP address range.

Parameter	Description
	• **depth** *num* – Specifies how many nodes within the geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify depth 2. By default, the full tree (all nodes) is displayed. • **directory** *num* – Displays entries for the specific geo-location database directory. • **top** *num* [**percent** [**global**]] – Display the top statistics for the selected geo-location database. • **statistics** – Displays client statistics for the specified geo-location.
file [*file-name*]	Displays the geo-location database files on the ACOS Device, and their load status. (Data from a geo-location database file does not enter the geo-location database until you load the file.
ip *ipaddr*	Displays geo-location database entries for the specified IP address. • **statistics** – Displays client statistics for the specified geo-location. • **policy** *policy-name* – Filter output by policy.
ipv6 *ipv6addr*	Displays geo-location database entries for the specified IPv6 address. • **statistics** – Displays client statistics for the specified geo-location. • **policy** *policy-name* – Filter output by policy.
rdt [*options*]	Displays aRDT data for geo-locations. You can use the following options: • **active** – Displays data for aRDT. • *geo-location-name* – Displays aRDT data only for the specified GSLB geo-location.

Parameter	Description
	• **site** *site-name* – Displays aRDT data only for the specified GSLB site. • **depth** *num* – Specifies how many nodes within the geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify **depth 2**. By default, the full tree (all nodes) is displayed.

Mode All

Usage The matched client IP address and the hits counter indicate the working status of the geo-location configuration.

Example The following command shows the status of a geo-location db named "pc":

```
ACOS# show gslb geo-location db arin
         Last = Last Matched Client, Hits = Count of Client
matched
         Sub = Count of Sub Geo-location
         T = Type, P-Name = Policy name
         G(global)/P(policy), S(sub)/R(sub range)
         M(manually config)/B(built-in)

Geo-location: arin
From    To/Mask          Last        Hits      Sub    T    P-Name
-----------------------------------------------------------------
                                      0         21    G

ACOS#
```

The following table describes the fields in the command output.

Field	Description
Geo-location	Name of the geo-location.

Field	Description
From	Beginning address in the address range assigned to the geo-location.
To	Ending address in the address range assigned to the geo-location.
Last	Client IP address that most recently matched the geo-location. If the value is “empty”, no client addresses have matched.
Hits	Total number of client IP addresses that have matched the geo-location.
Sub	Number of sublocations within the geo-location. For example, if you configure the following geo-locations, geo-location “pc” has two sublocations, “pc.office” and “pc.lab”. • geo-location pc 10.1.0.0 mask /16 • geo-location pc.office 10.1.1.0 mask /24 • geo-location pc.lab 10.1.2.0 mask /24
T	Type of geo-location: • G – The geo-location is configured at the global level in the ACOS Device configuration. • P – The geo-location is configured within a GSLB policy.
P-Name	Name of the GSLB policy where the geo-location is configured.

Example

The following command shows the load status information for a geo-location database file:

```
ACOS(config)# show gslb geo-location file test1
T = T(Template)/B(Built-in), Per = Percentage of loading
Filename      T Template           Per  Lines    Success
Error
-------------------------------------------------------------
-
test1         T t1                 98%  11       10       0
```

Example The following command displays entries in the geo-location database:

```
ACOS(config)# show gslb geo-location db

         Last = Last Matched Client, Hits = Count of Client
matched
         T = Type, Sub = Count of Sub Geo-location
              G(global)/P(policy), S(sub)/R(sub range)
              M(manually config)

Global
Name    From          To/Mask          Last             Hits
Sub  T
-------------------------------------------------------------------
--------
NA      (empty)       (empty)          (empty)          0
1    G

Geo-location: NA, Global
Name    From          To/Mask          Last             Hits
Sub  T
-------------------------------------------------------------------
--------
US      (empty)       (empty)          (empty)          0
10   GS

Geo-location: NA.US, Global
Name    From          To/Mask          Last             Hits
Sub  T
-------------------------------------------------------------------
--------
        69.26.125.0   69.26.125.255    (empty)          0
0    GR
        69.26.126.0   69.26.126.255    (empty)          0
0    GR
        69.26.127.0   69.26.127.255    (empty)          0
0    GR
...
```

show gslb group

Description Show information for GSLB controller groups.

Syntax

```
show gslb group
[brief | group-name [...] [statistics] | statistics]
```

brief	Show brief information GSLB group information.
group-name	Specify GSLB group name of length a maximum of 63 characters.
statistics	Show GSLB counters and statistics.
|	Specify output modifiers.

Default N/A

Mode All

Example The following commands add a GSLB controller to the default GSLB group, enable the device's membership in the group, and display group information:

```
ACOS(config)# gslb group default
ACOS(config-gslb group)# enable
ACOS(config-gslb group)# show gslb group brief
                      Pri = Priority, Attrs = Attributes
                          D = Disabled, L = Learn
                          P = Passive, * = Master
Name                              Pri Attrs Master
Member
-----------------------------------------------------------------
---------
default                           255 L*    local           2

ACOS-Active-gslb:Member# show gslb group
                      Pri = Priority, Attrs = Attributes
                      S-Cfg = Secure Config
                      S-State = Secure Status
```

```
                          D = Disabled, L = Learn
                          P = Passive, * = Master
                          E = Enabled, EF = Enable-Fallback
                          Unsec = Unsecure, Unkwn = Unknown
                          Estng = Establishing, Estd =
Established
Group: v4-v6, Master: 13.136
Member      Sys-ID   Pri Attrs  Status      S-Cfg S-State
Address
-------------------------------------------------------------
----------
local       123a0c29 100 L      OK          ab54c229 100 L*
Synced      E     Estd    3.3.3.136
ACOS(config-gslb group)# show gslb group
                      Pri = Priority, Attrs = Attributes
                          D = Disabled, L = Learn
                          P = Passive, * = Master
Group: default, Master: 192.168.101.72
Member                           Sys-ID   Pri Attrs  Status
 Address
-------------------------------------------------------------
----------
local                            825b1429 100 L      OK
192.168.1.131                    941a1229 100        Synced
192.168.1.132                    ab301229 100 P      Synced
```

```
ACOS(gslb:Master)# show run gslb group
!Section configuration: 76 bytes
!
gslb group default
  enable
  primary-ipv6 2001:204::3
  priority 255
!
ACOS(gslb:Master)# show gslb group
                      Pri = Priority, Attrs = Attributes
                      S-Cfg = Secure Config
                      S-State = Secure Status
                          D = Disabled, L = Learn
```

```
                          P = Passive, * = Master
                          E = Enabled, EF = Enable-Fallback
                          Unsec = Unsecure, Unkwn = Unknown
                          Estng = Establishing, Estd =
Established
Group: default, Master: local
Member    Sys-ID    Pri Attrs  Status      S-Cfg S-State Address
-------------------------------------------------------------
-------
local     cfdb6d29 255 L*     OK          2001:204::3 Idle D Unsec
ACOS1     818d7129 100 PL     Synced       D     Unsec
2001:204::4
```

The following table describes the fields in the command output.

Field	Description
Member	GSLB controllers currently in the group. The “local” member is the GSLB controller on which you entered this show command.
ID	Group member ID assigned by the controller group feature.
Pri	Priority of the GSLB controller.
Attrs	GSLB group attributes of the member: • D – Member is disabled. • L – Group learning is enabled on this member. • P – Member’s connection with this member (the member on which you enter the `show gslb group command`) is passive. The group connection between any two controller group members is a client-server connection. The group member that initiates the connection is the client, and has the passive side of the connection. The other member is the server. • * – Member is the current master for the group.

Field	Description
	NOTE: Attributes are displayed only when at least two group members are connected.
Status	When the GSLB group is starting up, this column shows the protocol status. After the group is established, this column shows the group status. Protocol status: • Unsec (unsecure) • Idle • Active • OpenSent • OpenConfirm • Established Group status of the member: • Ready • FullSync/MasterSync • Synced **NOTE:** If the group status of the member is OK, this ACOS Device (the one on which you entered the command) knows of the member, but no connection between this ACOS Device and the member is required.
S-Cfg	Secure configuration of IPv6 connection. Options: D, L , P, *
S-Stat	Secure status of the IPv6 connection. (Sec = Secure, Unsec = Unsecure)
Address	IPv4 or IPv6 address of GSLB group master or member devices.

```
ACOS-GSLB:Master# show gslb group statistics
                      CnOK = Connect Success, CnBad = Connect
Fail
                      OpIn = Open In, OpOut = Open Out, OpOK =
Open Success
                      SecOK = Secure Success, SecBad = Secure
Fail
                      HSOK = SSL Handshake Success, HSBad = SSL
Handshake Fail
                      SyncSn = Sync Sequence Number
Group: abcd, Master: local
Member CnOK  CnBad OpIn  OpOut OpOK  SyncSn  UpdIn  SecOK
SecBad HSOK  HSBad
----------------------------------------------------------------
----------
SITE     0      0        1       1      1       1       3       1
                0
```

Field	Description
Group	GSLB controllers group name. The “local” member is the GSLB controller on which you entered this show command.
Master	Group member ID assigned by the controller group feature.
Member	Priority of the GSLB controller.
CnOK	Connect Success. 0 = No 1= Yes
CnBad	Connect Fail. 0 = No 1= Yes
OpIn	Open In. 0 = No 1= Yes
OpOut	Open Out. 0 = No 1= Yes
OpOK	Open OK
SyncSn	Synchronize Sequence Number - 0, 1,2, 3
UpdIn	Update Initiate Status - 0,1,2,3
SecOK	Secure Connection Success; 0 = No 1= Yes

Field	Description
SecBad	Secure Connection Fail ; 0 = No 1= Yes
HSOK	SSL Handshake Success; 0 = No 1= Yes
HSBad	SSL Handshake Fail; 0 = No 1= Yes

show gslb ip-list

Description Display information for GSLB IP lists.

Syntax

```
show gslb ip-list
[brief | list-name | id num | ip ipaddr | statistics]
```

Mode All

show gslb memory

Description Display memory allocation information for GSLB.

Syntax

```
show gslb memory [mem-loc-id [...]] [interval seconds]
```

Mode All

Example

```
ACOS# show gslb memory
Type                  Allocated(#)          Alloc count
Free count    ID
-------------------------------------------------------------------
-----------------
DPlane                90                    100
10
  normal              2
                 0
  geo-location        5
                33
  IP range            73
                34
  string              6
                44
```

```
  IPC message          1
               45
  IPC msg node         1
               46
  file                 1
               49
  file error           1
               50
Total                  90
Total                  90
------------------------------------------------------------
-----------
Protocol               22                    24
2
  gmp instance         2
  IPC client           1
  IPC message          2
  log                  1
  thread               8
  thread master        1
  RDT arena            1
  link list            3
link node           2
  cache table          1
Total                  22
```

show gslb policy

Description Show GSLB metric settings for GSLB policies.

Syntax

```
show gslb policy [policy-name]
```

Mode All

The following table describes the fields in the command output.

Field	Description
Policy	Name of the GSLB policy.

Field	Description
name	
Type	Name of the GSLB metric.
MO	For GSLB metrics, indicates the order in which the metrics are used.
Option	Metric or option name.
En-Value	For metric, indicates whether they are enabled (yes or no). For options, indicates the value.
Description	Description of the metric or option.

show gslb protocol

Description Show the status of the GSLB protocol on the GSLB ACOS Device and the SLB devices and site ACOS Device.

Syntax

```
show gslb protocol [[geo-location-name] port  portnum]
```

Mode All

Usage When ACOS version is upgraded to 4.1.4-GR1, a GSLB controller sends a message to check the compatibility with GSLB version 1. Then the connection is re-attempted using GSLB version 2.
In ACOS version 5.0.0, you can enable secure GSLB protocol.

NOTE: For GSLB group member "**show gslb protocol**" output will show “None” for "**Secure Configuration**" and "**Current SSL State**" as it is under Group Control.

Example The following command examples show GSLB version and protocol status
information on an ACOS Device acting as a GSLB controller WITH IPv4 address:

```
ACOS# show gslb protocol
GSLB protocol is disabled for GSLB controller.
GSLB protocol is disabled for site devices.
```

Example GSLB controller WITH IPv6 address:

```
GSLB site: OLD272
SLB device: old-272-2500 (172.16.203.5:2974) Established
 Session ID:    4111
 Connection succeeded:                2 |Connection failed:
                0
 Open packet sent:                    2 |Open packet received:
                1
 Open session succeeded:              1 |Open session failed:
                1
 Sessions Dropped:                    0 |Update packet
received:             554
 Keepalive packet sent:             137 |Keepalive packet
received:          137
 Notify packet sent:                  0 |Notify packet
received:               1
 Message Header Error:                0 |Protocol RDT(ms):
                0
 GSLB Protocol Version:               1

GSLB site: 272P13
SLB device: 272p13-dev1 (172.16.203.5:18386) Established
 Session ID:    26323
 Connection succeeded:                1 |Connection failed:
                0
 Open packet sent:                    1 |Open packet received:
                1
 Open session succeeded:              1 |Open session failed:
                0
 Sessions Dropped:                    0 |Update packet
received:             554
 Keepalive packet sent:             137 |Keepalive packet
received:          137
 Notify packet sent:                  0 |Notify packet
received:               0
 Message Header Error:                0 |Protocol RDT(ms):
                0
 GSLB Protocol Version:               2 |Peer ACOS Version:
   2.7.2-P13 Build 48

GSLB site: 414gr1
```

```
SLB device: 414gr1-shared1 (172.16.203.5:18386) Established
 Session ID:    14901
 Connection succeeded:                1 |Connection failed:
                0
 Open packet sent:                    1 |Open packet received:
                1
 Open session succeeded:              1 |Open session failed:
                0
 Sessions Dropped:                    0 |Update packet
received:             554
 Keepalive packet sent:             137 |Keepalive packet
received:          137
 Notify packet sent:                  0 |Notify packet
received:               0
 Message Header Error:                0 |Protocol RDT(ms):
                0
 GSLB Protocol Version:               2  Peer ACOS Version:
   4.1.4-GR1 Build 81

GSLB site: 5.0.0
SLB device: 5.0.0(172.16.203.5:1962) Established
 Session ID:    50825
Secure Config                    Enable |Current SSL State
   Secure - Established
 Connection succeeded:                1 |Connection failed:
                0
 Open packet sent:                    1 |Open packet received:
                1
 Open session succeeded:              1 |Open session failed:
                0
 Sessions Dropped:                    0 |Update packet
received:             550
 Keepalive packet sent:             137 |Keepalive packet
received:          136
 Notify packet sent:                  0 |Notify packet
received:               0
 Message Header Error:                0 |Protocol RDT(ms):
                0
 GSLB Protocol Version:               2 |Peer ACOS Version:
   5.0.0 Build 44
```

```
Secure negotiation Success:      1 | Secure negotiation Failures:
           0
 SSL handshake Success:                1 |SSL handshake
Failures:               0
```

Field	Description
Secure Config	(Enable / Disable / Enable-Fallback) – Provides the configured secure setting for a peer GSLB device. It is based on global and per-partition config of that peer.
Current SSL State	(Unsecure /Secure – Establishing / Secure – Established) – It shows the current SSL state of the peer connection.
Secure negotiation Success	This count increments when both devices support secure and open message negotiation succeeds.
Secure negotiation Failures	This count increments when one device is secure enabled and other device is secure disabled – Secure Negotiation Failure case.
SSL handshake Success	After both devices negotiate to establish secure channel and after SSL Handshake is successful, it is incremented.
SSL handshake Failures	Counter for after both devices negotiate to establish secure channel but connection fails during SSL handshake due to any SSL related issue.

show gslb rdt

Description Show aRDT data.

Syntax

```
show gslb rdt

[geo-location
  [active [geo-location-name...]
          [site site-name] [depth num]]

[slb-device
  [active [geo-location-name...]
          [ip ipaddr | ipv6 ipv6addr [...]]] |
local-info]
```

Parameter	Description
geo-location	Displays aRDT data based on geo-location. Optional parameter includes: • **active** – Displays data for aRDT. Optional parameter modifiers include: ◦ *geo-location-name* – Displays aRDT data only for the specified GSLB geo-location. ◦ **site** *site-name* – Displays aRDT data only for the specified GSLB site. ◦ **depth** *num* – Specifies how many nodes within the geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify **depth 2**. By default, the full tree (all nodes) is displayed.
slb-device	Displays aRDT data based on SLB device. Optional parameter includes: • **active** – Displays data for aRDT. Optional parameter modifiers include: ◦ *device-name* – Displays aRDT data only for the specified device. ◦ **ip** *ipaddr* [...] – Displays aRDT data only for the specified clients. By default, the full tree (all nodes) is displayed. ◦ **ipv6** *ipaddr* [...] – Displays aRDT data only for the specified clients. By default, the full tree (all nodes) is displayed.

Mode All

Usage All of the options except **local-info** are applicable when you enter the command on a GSLB ACOS Device. To display local aRDT data on a site

ACOS Device, enter the command on the site ACOS Device and use the **local-info** option.

Example

Here is an example of the output for this command when entered on the GSLB ACOS Device:

```
ACOS# show gslb rdt
TTL = Time to live(Unit: min), T = Type, A(active)
Device: site1/remote
IP              TTL   T|      1      2      3      4      5      6
  7      8
-----------------------------------------------------------------
----------------
10.10.10.2      10    A|      0      0      0      0      0      0
  0      0
20.20.20.21     10    A|     41     40     29     46     38     42
 34     30
192.168.217.1   10    A|     38     54     46     50     43     38
192.168.217.11  10    A|     41     40     29     46     38     42
 34     30

Device: site2/local
IP              TTL   T|      1      2      3      4      5      6
  7      8
-----------------------------------------------------------------
----------------
10.10.10.2      10    A|     35     52     35     40     54     56
 44     48
20.20.20.21     10    A|     20     20     16     16     20     16
 20     18
192.168.217.1   10    A|     16     44     20     16     20     18
192.168.217.11  10    A|     20     20     16     16     20     16
 20     18

                T = Type: A(active), TS = Time Stamp(unit:
min)

Geo-location                          Site
       T RDT TS
```

```
-----------------------------------------------------------------
----------------
cn.sh                                    site1
       A 38   10
                                         site2
       A 18   10
cn.bj                                    site1
       A 30   10
                                         site2
       A 18   10
jp                                       site1
       A 30   10
                                         site2
       A 18   10
us                                       site1
       A 0    10
                                         site2
       A 48   10
```

aRDT show command output for IPv6 address.

```
For example:
73-83-gslb:Master# show gslb rdt controller active
                Age = Aging Time(Unit: min), T = Type, A
(active)

Site: ACOS-272
IP              Age    T|      1      2      3      4      5      6
  7      8
2001:201::3     8      A|     16     16     16     16     16     16
 16     16
Site: ACOS-272p13
IP              Age    T|      1      2      3      4      5      6
  7      8
2001:201::3     8      A|     26     25     24     23     22
Site: ACOS-414gr1
IP              Age    T|      1      2      3      4      5      6
  7      8
2001:201::3     8      A|     16     16     16     16     16     16
 16     16
```

This example shows the default display (with no additional options). The TTL results are organized by site ACOS Device, then by geo-location.

The following table describes the fields in the command output.

Field	Description
Device	Site ACOS Device.
IP	IP (IPv4 or IPv6) address at the other end of the aRDT exchange.
TTL	Time-to-live for the Active-TT entry.
T	RDT type, which can be A (aRDT).
1-8	Individual aRDT measurements (in units of seconds).
Geo-location	Geo-location name for which aRDT measurements have been taken.
Site	GSLB site name within the geo-location.
T	RDT type. (See descriptions above.)
RDT	Individual aRDT measurements (in units of seconds).
TS	System time stamp of the aRDT measurement.

show gslb samples conn

Description Show the number of connections that are currently on a virtual port.

Syntax

```
show gslb samples conn
[service-name | vipaddr]
[port  port-num]
[range range-start range-end]
```

Parameter	Description
service-name | *vipaddr*	Specifies the service name or service IP.
port-num	Specifies the virtual port.
range-start	Specifies the range start.
range	Collects samples only for the specified range of

Parameter	Description
range-start *range-end*	service port numbers.

Mode All

Usage The number of connections on the site is sampled based on the GSLB status interval. This is configurable using the gslb protocol command. Samples are listed row by row. The first 7 samples appear on row 1, the second 7 samples appear on row 2, and so on.

If you disable the GSLB protocol, the data is cleared.

Example The following example shows connection activity for virtual port 80 on virtual server “china”.

```
ACOS# show gslb samples conn china 80
0         | 1          2          3          4          5          6
          7
-------------------------------------------------------------------
--------------
1         | 15000      25000      35000      45000      55000
65000      75000
2         | 85000      95000      105000
```

show gslb samples conn-load

Description Show the number of connections on each virtual server.

Syntax

```
show gslb samples conn-loadnum-samplesinterval
  [service-name | vipaddr]
  [port-num]
```

Parameter	Description
num-samples	Number of connection-load samples to collect and display.
num-samples	Number of seconds to wait between collection of each sample.

Parameter	Description
service-name | *vipaddr*	Collects samples only for the specified service IP.
port-num	Collects samples only for the specified service port number.

Mode All

Example The following command shows 5 connection-load samples, collected at 5-second intervals:

```
ACOS# show gslb samples conn-load 5 5
ip1:80, average is: 36
         | 1         2         3         4         5         6
        7
-------------------------------------------------------------------
--------------
1        | 0         0         11        1         168

ip2:80, average is: 38
         | 1         2         3         4         5         6
        7
-------------------------------------------------------------------
--------------
1        | 0         0         22        2         168

ip3:80, average is: 60
         | 1         2         3         4         5         6
        7
-------------------------------------------------------------------
--------------
1        | 120       0         0         0         180

ip4:80, average is: 86
         | 1         2         3         4         5         6
        7
-------------------------------------------------------------------
--------------
1        | 240       0         0         0         192
```

In this example, five samples, taken at 5-second intervals, are shown for each of four services (ip1:80 to ip4:80). Services are listed by service IP and service port.

In each section, the numbers across the top are column numbers. The numbers along the leftmost column are row numbers. The other numbers are the actual connection load data. For example, for ip1:80 (service port 80 on service IP "ip1"), there were no connections during the first or second data samples, and 11 connections during the third sample.

show gslb samples rdt

Description Show the aRDT between the GSLB ACOS Device and a client for a geo-location, slb-device, or GSLB controller.

Syntax

```
show gslb samples rdt

[geo-location
  [active [geo-location-name ...]
          [site site-name] [depth num]]

[slb-device
  [active [geo-location-name ...]
          [device-name] [ip ipaddr] | [ipv6 ipv6addr]]
[controller [active [geo-location-name ...] [device-name] [ip
ipaddr] | [ipv6 ipv6addr]]
```

Parameter	Description
geo-location	Displays aRDT data based on geo-location. Optional parameter includes: • **active** – Displays data for aRDT. Optional parameter modifiers include: • *geo-location-name* – Displays aRDT data only for the specified GSLB geo-location. • **site** *site-name* – Displays aRDT data only for the specified GSLB site. • **depth** *num* – Specifies how many nodes within the

Parameter	Description
	geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify **depth 2**. By default, the full tree (all nodes) is displayed.
slb-device	Displays aRDT data based on SLB device. Optional parameter includes: • **active** – Displays data for aRDT. Optional parameter modifiers include: • *device-name* – Displays aRDT data only for the specified device. • **ip** *ipaddr* – Displays aRDT data only for the specified clients. • **ipv6** *ipv6addr* – Displays aRDT data only for the specified clients. By default, the full tree (all nodes) is displayed.

Mode All

Usage Eight aRDT samples are displayed for each device. Times are shown in 10-millisecond (ms) increments. In the example below, the first aRDT time for Device1 is 50 ms.

If you disable the GSLB protocol, the data is cleared.

show gslb service

Description Show the configuration information for services.

Syntax

```
show gslb service
{cache | dns-a-record | dns-caa-record |dns-cname-record |
dns-mx-record | dns-ns-record | dns-ptr-record | dns-srv-
record | dns-txt-record | session}
[service-name ...] [zone zone-name]
[ip ipaddr {subnet-mask | /mask-length}]
```

Parameter	Description
cache	Displays service information in the GSLB DNS cache.
dns-a-record	Displays Address records for GSLB services.
dns-caa-record	Displays Certification Authority Authorization records for GSLB services.
dns-cname-record	Displays CNAME records for GSLB services.
dns-mx-record	Displays MX records for GSLB services.
dns-ns-record	Displays name server records for GSLB services.
dns-ptr-record	Displays pointer records for GSLB services.
dns-srv-record	Displays service records for GSLB services.
dns-txt-record	Displays service records for GSLB services.
session	Displays current GSLB sessions for services.
service-name	Specifies a service name.
zone *zone-name*	Specifies a zone name.
ip *ipaddr* {*subnet-mask* | */mask-length*}	Specifies a client host or subnet address. (This option applies only to the session option.)

Mode All

Example The following example shows CNAME information for zone “example.com”:

```
ACOS# show gslb service dns-cname-record example.com
Zone: example.com
                                Alias = Alias Name, Geoloc =
Geo-location
                                G-Geoloc = Matched Global Geo-
location
                                P-Geoloc = Matched Policy Geo-
location
Service      Alias                          Geoloc       G-
Geoloc     P-Geoloc
-----------------------------------------------------------------
--------------
http:www     http.example.com                pc1
(empty)      (empty)
ftp:ftp      ftpp.example.com                pc1
(empty)      pc1
```

Example The following example shows CAA information for zone "a10-black.com":

```
ACOS# show gslb service dns-caa-record example.com
Zone: a10-black.com
Service Flags Tag Value Hits
-----------------------------------
www.a10-black.com:http
geo.a10-black.com:5566 2 iodef a10-white.com
2 issue a10networks.com
23 issuewild a10networksss.com
```

The following table describes the fields in the command output.

Parameter	Description
Service	Service type and service name.
Flag	Issuer Critical Flag.
Tag	Property tag.

Parameter	Description
Value	Rdata.
Hits	Number of times the service IP was selected.

show gslb service-group

Description Shows FQDN group information.

Syntax

```
show gslb service-group group-name
[
cache |
dns-a-record |
dns-cname-record |
dns-mx-record |
dns-ns-record |
dns-ptr-record |
dns-srv-record |
dns-txt-record |
dns-caa-record |
session [ip ipaddr | ipv6 ipv6addr] |
site-stat
]
```

Mode All

show gslb service-ip

Description Shows information for a GSLB service.

Syntax

```
show gslb service-ip
{service-name | vipaddr | local-info | statistics}
```

Parameter	Description
service-name | *vipaddr*	Specifies the service name or VIP address.
local-info	Shows local SLB virtual-server information.
statistics	Shows GSLB statistics for the service-IP.

Example The following command shows information for vip1:

```
ACOS(config-service-ip:vip1)#  show gslb service-ip
P-Cnt = Count of Service Ports, Attrs = Attributes
V = Is Virtual Server, D = Disabled
P = GSLB Protocol,     L = Local Protocol
M = Manually Health Check, * = Dynamic
S = Shared Virtual Server
Service-IP                                      IP/Desc         Attrs State
P-Cnt Hits
-------------------------------------------------------------------------------
------------------------
:d1:vip4                                        10.20.11.14     V     DOWN
2     0
:d1:vip3                                        25.100.100.102  VP    UP
1     1
:d2:vip2                                        25.100.100.101  VP    UP
1     2
:d2:vip1                                        25.100.100.100  VPS   UP
1     0
```

The following table describes the fields in the command output.

Field	Description
Service-IP	Device name and service IP name.
IP	IP address of the service.
V	Indicates whether the service IP is a virtual server IP address (Y) or a real server IP address (N).
E	Indicates whether the service IP is enabled.
State	Indicates the service IP state: UP or DOWN.
P-Cnt	Number of service ports on the service IP.
Hits	Number of times the service IP has been selected.
S	Indicates whether the service IP is shared between multiple SLB devices. **Note:** Virtual IP servers marked as shared 'S' will not accurately show the disabled state under this command.

show gslb service-port

Description Show information about the GSLB service ports configured on the sites.

Syntax

```
show gslb service-port [local-info]
```

The **local-info** parameter displays local SLB virtual-port information.

Mode All

Example The following command shows information about all the configured GSLB service ports.

```
ACOS# show gslb service-port
                Attrs = Attributes, A-Svr = Active Real
Servers
                Cur-Conn = Current Connections
                 D = Disabled, P = GSLB Protocol, L = Local
Protocol
                 T = TCP, M = Manually Health check, * =
Dynamic
Service-Port              Attrs State      Act-Svrs   Cur-Conn
-------------------------------------------------------------
-----
10.77.27.222:80           L     DOWN       0          0
10.10.10.1:80                   DOWN       0          0
67.67.6.84:80                   UP         1          0
67.67.6.82:21                   UP         1          0
192.168.100.6:80                DOWN       0          0
```

The following table describes the fields in the command output.

Field	Description
Service-Port	Service IP address and service port number.
Attrs	Indicates whether the service port is reached using the GSLB protocol or the local (SLB) protocol.
State	Indicates the service state: UP or DOWN.

Field	Description
	Note: Virtual IP servers marked as shared 'S' will not accurately show the disabled state under this command.
Act-Svrs	Number of active real servers for the service.
Cur-Conn	Current number of aggregated connections at the port level.

show gslb session

Description Show cached GSLB policy selections.

Selections are cached on a zone:service basis. While a cached GSLB policy selection is valid (that is, before it ages out), the cached selection is used for subsequent requests from the same client for the same zone and service.

Syntax

```
show gslb session
[service-name ...] [zone zone-name]
[ip ipaddr {subnet-mask | /mask-length}]
[ipv6 ipv6addr {subnet-mask | /mask-length}]
[match domain-name]
```

Parameter	Description
service-name	Specifies a service name.
ip *ipaddr* {*subnet-mask* | */mask-length*}	Specifies a client host or subnet address.
match	Specifies a domain name to match to when displaying session information.
zone *zone-name*	Specifies a zone name.

Mode All

Example The following command shows the GSLB session information for DNS sticky with ECS :

```
ACOS # show gslb session
```

```
Best = Best Service-IP for sticky
TTL = DNS TTL, Time until next query(unit: min)
Update = Update Time(unit: sec), Aging = Aging Time(unit: sec)
Last = Hits of Last one second
Type = (E) ECS
Service: www.example.com:0
Total Number of Sessions: 2
Client           Subnet   Best            Mode        Hits/Last
TTL       Update Aging   Type
-------------------------------------------------------------
-----------------------------------
10.214.4.2       /32      10.1.1.100      Server         1/1
71582784  566    409
1.1.1.0          /24      10.1.1.100      Server         1/1
71582787  756    599      E
Matched: 2
```

The following table describes the fields in the command output.

Field	Description
Service	Service type and service name.
Total number of sessions	Number of GSLB sessions configured.
Client	Specific client IP address/ server.
Subnet	Subnet mask type used.
Best	Best service IP match for sticky.
Mode	Type of mode.
Hits	Number of times the service IP was matched.
Last TTL	Most recent time the TTL record was used.
Update	Update time in seconds.
Aging	Aging time in seconds.
Type	Indicates if EDNS client subnet is enabled (E) or disabled.

show gslb site

Description Show GSLB site information.

Syntax

```
show gslb site [site-name ...] [bw-cost] [fqdn-based] [curr-conn] [statistics]
```

Parameter	Description
site-name	Displays information only for the specified site.
bw-cost	Displays BW-Cost information.
fqdn-based	Displays Fully-Qualified Domain Name (FQDN) based details.
curr-conn	Displays the aggregated current connection count for the site.
statistics	Displays statistics.

Mode All

Example The following command shows information for GSLB site “Site1”:

```
ACOS# show gslb site Site1
Site          Device/server    VIP        Service            State
          Hits
-------------------------------------------------------------------
---------------------
Site1         Device1 (device) 2.1.1.10                      AllUp
          20
            1.2.2.2                      80:TCP:http       Up

                                         53:UDP:dns        Up

                               2.1.1.11  80:TCP:gitlab     Up
          0
            serverB (server)                               Up
        10
            3.1.1.10                     80:TCP:http       Up
                                         53:UDP            Up
```

```
                                                80:TCP:gitlab     Down
          0
```

The following table describes the fields in the command output.

Field	Description
Site	GSLB site name.
Device/server	Device name and device IP address or real server name and real server IP address.
VIP	Virtual IP address for the service.
Service	Port, protocol, and the associated services.
State	Virtual port state.
Hits	Number of times the service IP was selected.

The following table describes the fields in the command output when the **bw-cost** option is used.

Field	Description
Site	GSLB site name.
Template	SNMP template name.
Current	Current value of the SNMP object used for measurement.
Highest	Highest value of the SNMP object used for measurement.
Limit	Limit configured for the BW-Cost metric.
U	Indicates whether the site is usable, based on the BW-Cost measurement.
Type	Data type of the SNMP object.
Len	Data length of the SNMP object.
Value	Value of the SNMP object.
TI	Time interval between measurements.

Example The following command shows GSLB site statistics:

```
ACOS# show gslb site statistics
```

```
Site                                Hits                Last

-------------------------------------------------------------------
-----
site1                               14                  2.1.1.10

site2                               0                   (empty)

site3                               0                   (empty)

site4                               0                   (empty)
```

The following table describes the fields in the command output when the **statistics** option is used.

Field	Description
Site	GSLB site name.
Hits	Number of times the site was selected.
Last	Site that was most recently selected.

Example The following command shows the FQDN information for GSLB site "Site1":

```
ACOS # show gslb site s1 fqdn-based
GSLB Site Device/Server VIP Vport State Hits
-------------------------------------------------------------------
-------------------------------------
s1 PartUp 0
d1 (device)
DRD-10.1.1.3-ser AllUp
ver.geo.com (de 1.1.1.1 Up 0
vice) 10.1.1.100 Up 0
10.1.1.3
```

The following table describes the fields in the command output:

Field	Description
Site	GSLB site name.

Field	Description
Device/Server	Device name and device IP address or real server name and real server IP address.
VIP	Virtual IP address for the service.
Vport	Virtual port number.
State	Virtual port state.
Hits	Number of times the service IP was selected.

Example The following command shows the current connection information for GSLB site “Test”:

```
ACOS(config)#show gslb site curr-conn
GSLB Site     Device/Server    VIP          Service      State
       Curr-Conn
-------------------------------------------------------------------
-----------------------------------
Test
              d1 (device)
              10.2.1.1         x.x.x.x

                                            80:TCP       Up
       1000
              D2 (device)
              10.2.1.2         x.x.x.x
                                            80:TCP       Down
       771
```

The following table describes the fields in the command output when the **curr-conn** option is used.

Field	Description
Site	GSLB site name.
Device/Server	Device name and device IP address or real server name and real server IP address.
VIP	Virtual IP address for the service.

Field	Description
Service	Port, protocol, and the associated service.
State	Virtual port state.
Hits	Number of times the service IP was selected.
Curr-Conn	The aggregated number of current connections for the site.

show gslb slb-device

Description Show information about an SLB device used by GSLB.

Syntax

```
show gslb slb-device
[
device-name  [fqdn-based]|
local-info |
rdt active [device-name ... | ip ipaddr ...]
]
```

Parameter	Description
device-name	Displays information only for the specified SLB device. The parameter includes: • `device-name` - Displays SLB device name. • `fqdn-based` - Displays fully-qualified domain name (fqdn) based view by device.
local-info	Displays local SLB device information on a site SLB device.
rdt *options*	Displays aRDT data based on SLB device. Optional parameter includes: **active** – Displays data for aRDT. Optional parameter modifiers include: • *device-name* – Displays aRDT data only for the specified device.

Parameter	Description
	• **ip***ipaddr*[...] – Displays aRDT data only for the specified clients. By default, the full tree (all nodes) is displayed.

Mode All

Example The following command shows information about SLB device “Device1”:

```
ACOS# show gslb slb-device Device1 fqdn-based
Attrs = Attributes, APF = Administrative Preference,
Sub-Cnt = Count of Service-IPs
Sesn-Uzn = Session Utilization
Sesn-Num = Number of Available Sessions
Device IP Attrs APF Sesn-Uzn Sesn-Num Sub-Cnt
------------------------------------------------------------
------------------
site1:Device1 1.2.2.2 L 200 0% 0 3
site1:DRD-10.1.1.3-server.geo.com 10.1.1.3 P 100 200 0% 2
```

The following table describes the fields in the command output.

Field	Description
Device	Site name and device name.
IP	SLB device’s IP address.
Attrs	Attributes of the device.
APF	Administrative preference for the device.
Sesn-Uzn	Current session utilization on the device.
Sesn-Num	Number of sessions available on the device.
Sub-Cnt	Number of service IPs on the device.

show gslb state

Description Show GSLB state information collected by GSLB debugging.

Syntax

```
show gslb state
```

Mode All

Usage To collect state information, enable GSLB debugging and use the **state** option. (See the example below.)

Example The following commands enable GSBL debugging with retention of state information, and initiate display of the state information:

```
site-acos-1(config)# debug gslb state
site-acos-1(config)# show gslb state
```

show gslb statistics

Description Show statistics for the GSLB protocol, for sites, or for zones.

Syntax **show gslb statistics** {**message** | secure | **site** | **zone**}

Mode All

Usage The **show gslb statistics message** command shows the same output as the **show gslb protocol** command. Similarly, the **show gslb statistics site** command shows the same output as the **show gslb site statistics** command, and the **show gslb statistics zone** command shows the same output as the **show gslb zone statistics** command.

Example The following command shows statistics for the GSLB protocol:

```
ACOS# show gslb statistics message
GSLB site: site1
    slb-dev: remote (20.20.20.2) Established
 Session ID:   40576
 Connection success:                    4 |Connection failure:
                  0
 Open packet sent:                      4 |Open packet
received:                  1
 Open session success:                  1 |Open session
failure:                  3
 Dropped sessions:                      0 |Update packet
received:             5101
```

```
 Keepalive packet sent:                1219 |Keepalive packet
received:          1218
 Notify packet sent:                      0 |Notify packet
received:                0
 Message Header Error:                    0 |
                  0

GSLB site: site2
    slb-dev: local (192.168.217.2) Established
 Session ID:   104
 Connection success:                      1 |Connection failure:
                  1
 Open packet sent:                        1 |Open packet
received:                  1
 Open session success:                    1 |Open session
failure:                  0
 Dropped sessions:                        0 |Update packet
received:               22
 Keepalive packet sent:                   2 |Keepalive packet
received:             1
 Notify packet sent:                      0 |Notify packet
received:                0
 Message Header Error:                    0 |
                  0

GSLB controller: 192.168.217.2 Established
 Session ID:   104
 Connection success:                      0 |Connection failure:
                  0
 Open packet sent:                        1 |Open packet
received:                  1
 Open Sent                                1 |Open session
failure:                  0
 Dropped sessions:                        0 |Update packet sent:
                 22
 Keepalive packet sent:                   2 |Keepalive packet
received:             1
 Notify packet sent:                      0 |Notify packet
received:                0
```

```
Message Header Error:                    0 |
                    0
```

show gslb statistics secure

Description Display statistics for all secure SSL contexts present on GSLB group, count of total SSL contexts currently present on box

Syntax

```
show gslb statistics secure
```

Default NA

Mode Global Configuration mode

Usage To view number of SSL contexts created when a GMP (controller, device, group) is enabled, and also a new context is created each time per-partition certificate or key is configured under "`gslb secure-attributes`"
configuration. This counter can be used to check any memory leaks occurring due to contexts retained on box even after configurations are removed.

NOTE: Context is cleared only after configurations are removed and also all the prior connections on this context are closed.

Example

```
ACOS(config)# show gslb statistics secure
Current SSL Contexts:   3
```

show gslb zone

Description Shows GSLB zone information.

Syntax

```
show gslb zone [zone-name]
[dns-info | dns-mx-record | dns-ns-record | dns-soa-record |
service-matching-rules | site | statistics ]
```

Parameter	Description
zone-name	Displays information only for the specified zone.
dns-info	Displays the DNS information for the zone.
dns-mx-record	Displays the MX records for the zone(s).
dns-ns-record	Displays the name server records for the zone(s).
dns-soa-record	Displays the start-of-authority records for the zone(s).
service-matching-rules	Displays the service matching rules configured for the zone(s).
site	Displays statistics for the zone(s) by related site.
statistics	Displays statistics for the zone(s).

Mode All

Example The following example shows information for zone *example.com*:

```
ACOS(config)# show gslb zone example.com
Zone            Service           Policy         TTL
State
-------------------------------------------------------------------
-------------------------
example.com                       default        10
FncUp
                http:www          pol_a10        10
PrtUp
                http:www-view-cl1 pol_a10        10        Down
                http:www-view-cl2 pol_a10        10
PrtUp
                http:www-view-cl3 pol_a10        10        Down
```

The following table describes the fields in the command output.

Field	Description
Zone	Zone name.
Service	Service type and service name.
Policy	GSLB policy name.
TTL	DNS TTL value set by GSLB in DNS replies to queries for the zone address.
State	State of the zone or zone-service. A zone can have the following states: **AllUp/FncUp/Down** A zone-service can have the following states: **AllUp/PrtUp/Down**

Example The following command shows MX records for zones:

```
ACOS# show gslb zone dns-mx-record
Pri = Priority,  Last = Last Server
Owner                    MX-Record                Pri    Hits
  Last
-------------------------------------------------------------------
----------
mail.abc.com:smtp        mail1.abc.com            0      0
                         mail2.xyz.com            10
```

The following table describes the fields in the command output.

Field	Description
Owner	Zone and service name to which the MX record belongs.
MX-Record	Name of the MX record.
Pri	Priority (preference) set for the MX record.
Hits	Number of times the record has been used.
Last	Most recent time the record was used.

Example The following command shows GSLB zone statistics:

```
ACOS(config-gslb zone-gslb service)# show gslb zone
example.com statistics
GSLB Zone example.com:
Total Number of Services configured: 1
               Rcv-query = Received Query, Sent-resp = Sent
Response
                   M-Proxy = Proxy Mode, M-Cache = Cache Mode
                   M-Svr = Server Mode,  M-Sticky = Sticky
Mode
                   M-Backup = Backup Mode
Service       Rcv-query  Sent-resp  M-Proxy M-Cache  M-Svr M-
Sticky M-Backup
-------------------------------------------------------------
-------------
http:www      0          0          0        0        0
12       0
Total         0          0          0        0        0
12       0
```

The following table describes the fields in the command output.

Field	Description
GSLB Zone	Zone name.
Total Number of Services configured	Number of GSLB services configured for the zone.
Service	Service type and service name.
Rcv-query	Number of DNS queries received for the service.
Sent-resp	Number of DNS replies sent to clients for the service.
M-Proxy	Number of DNS replies sent to clients by the ACOS Device as a DNS proxy for the service.
M-Cache	Number of cached DNS replies sent to clients by the ACOS Device for the service. (applies only if the DNS cache option is enabled in the policy.)
M-Svr	Number of DNS replies sent to clients by the ACOS

Field	Description
	Device as a DNS server for the service. (This statistic applies only if the DNS server option is enabled in the policy.)
M-Sticky	Number of DNS replies sent to clients by the ACOS Device to keep the clients on the same site. (This statistic applies only if the DNS sticky option is enabled in the policy.)
M-Backup	Number of DNS replies sent to clients by the ACOS Device using a backup record.

Example The following command shows dns info for the zone:

```
ACOS# show gslb zone a10-black.com dns-info
Zone:a10-black.com
--------------------------------------------------
$TTL 10
a10-black.com IN SOA ttl. exit. (777450 3600 900 1209600 10)
a10-black.com IN CAA 0 0 iodef a10-white.com
a10-black.com IN CAA 0 1 unknown a10-unknown.com
geo.a10-black.com IN CAA 2 iodef a10-white.com
geo.a10-black.com IN CAA 2 issue a10networks.com
geo.a10-black.com IN CAA 23 issuewild a10networksss.com
```

Example The following command shows service matching rules configured in the specified zone:

```
ACOS(config)# show gslb zone a10.com service-matching-rules
GSLB Zone a10.com:
Rule matching enabled, Hit count disabled
Total number of Valid SMRules: 2
Rule Target-Service       Hit
-------------------------------------------------------------
-------------------
1    www-view-cl1         0
2    www-view-cl2         0
```

The following table describes the fields in the command output.

Field	Description
GSLB Zone	The GSLB zone for which the service matching rules are displayed.
Rule matching	Indicates rule matching status for the specified GSLB zone. The possible values are **enabled** or **disabled**.
Hit count	Indicates the hit count feature status. The possible values are **enabled** or **disabled**. This feature is enabled when the **`hitcount-enable`** parameter under **`gslb service-matching-rules zone`** is set.
Total number of Valid SMRules	The total number of valid service matching rules (SMRules) configured in the specified GSLB zone. A rule is considered valid if it contains at least one condition and a target service.
Rule	Indicates the rule number for each service matching rule.
Target-Service	The target zone service configured for each rule.
Hit	Indicates the number of times each rule has been matched.

Example

The following command shows the service matching rules for all available zones:

```
ACOS(config)# show gslb zone service-matching-rules
GSLB Zone a10.com:
Rule matching enabled, Hit count enabled
Total number of Valid SMRules: 2
Rule Target-Service       Hit
-------------------------------------------------------------
-------------
1    www                  7
2    www-view-cl1         0
GSLB Zone google.com:
```

```
No service-matching-rules configured.
GSLB Zone example.com:
Rule matching enabled, Hit count disabled
Total number of Valid SMRules: 4
Rule Target-Service       Hit
-------------------------------------------------------------------
-------
1    www-view-1           0
2    www-view-2           0
3    www-view-3           0
4    www                  0
```

The fields in the command output are the same as those mentioned in Service Matching Rule fields.

clear gslb

Description Clear statistics or reset functions. Sub-command parameters are required for specific sub-commands.

Syntax

```
clear gslb {options}
```

Options	Description
all	Clears all GSLB statistics.
cache	Clears the GSLB DNS cache.
debug	Clears debug statistics.
fqdn	Clears FQDN statistics.
geo-location	Clears geo-location statistics.
group	Clears GSLB group statistics.
ip-list	Clears IP-list statistics.
memory	Clears memory statistics.
protocol	Clears GSLB protocol statistics.
rdt	Clears RDT samples.
samples	Clears aRDT samples.

Options	Description
server	Clears server statistics.
service	Clears service statistics.
service-group	Clears service group statistics
service-group-session	Clears service-group-session statistics
session	Clears GSLB sessions.
site	Clears site statistics.
slb-device	Clears SLB device samples.
statistics *options*	Clears message, site, or zone statistics.
zone [all | *zone-name* **] [service-matching-rules]**	Clears zone statistics for all GSLB zones or for the specified zone. Specify the **service-matching-rules** parameter to clear the service-matching rule hit count for all GSLB zones or the specified zone.

Server Load Balancing

ACOS Server Load Balancing (SLB) shares and distributes the load among multiple servers, thus improving throughput and performance beyond the capabilities of any single server. It provides fault tolerance and redundancy. Distributing the load among multiple devices enables more network reliability in the event that one server becomes unavailable.

This reference lists the CLI configuration and show commands that apply specifically to SLB.

Configuration Commands

health monitor

The health external command is accessed from Global Configuration mode, which is accessed by entering the **health monitor** command.

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)#
```

For more information about health monitors, see the “Health Monitoring” section of the *Application Delivery Controller Guide*.

default-state-up

Description Allows the initial default health state to be UP.

Syntax

```
[no] default-state-up
```

Default Disabled

Mode Health monitor configuration

Example The following command is the configuration example:

```
ACOS(config)# health monitor test_monitor
ACOS(config-health:monitor)# default-state-up
```

```
ACOS(config-health:monitor)#
```

disable-after-down

Description Disable the target of a health check if the target fails the health check. The server, port, or service group remains disabled until explicitly enabled.

Syntax

```
[no] disable-after-down
```

Default Disabled

Mode Health monitor configuration

Usage This command applies to servers, ports, or service groups using the health monitor. When a server, port, or service group is disabled based on this command, the server, port, or service group state is changed to `disable` in the running-config. If you save the configuration while the server, port, or service group is disabled, the state change is written to the startup-config.

Example The following command is the configuration example:

```
ACOS(config)# health monitor test_monitor
ACOS(config-health:monitor)# disable-after-down
ACOS(config-health:monitor)#
```

dsr-l2-strict

Description In Layer 2 DSR environments, this option ensures health check packets are only sent to servers in the same Layer 2 network as the ACOS device. The health check marks servers not in the same Layer 2 network as DOWN.

Syntax

```
[no] dsr-l2-strict
```

Default Disabled

Mode Health monitor configuration

Example The following command is the configuration example:

```
ACOS(config)# health monitor test_monitor
ACOS(config-health:monitor)# dsr-l2-strict
```

```
ACOS(config-health:monitor)#
```

header-insert

Description Configure the customize request header insertion for SIP method heath monitoring.

Syntax

```
[no] header-insert name:value
```

Default Not configured.

Mode Health monitor configuration

Usage This command applies only to health monitor method SIP. This configuration allows customizing request header content, which will append the SIP health check request header after the original header. The existing headers are not overwritten.

A maximum of eight lines of header-insert fields can be configured and the header content format should be *name:value* pair. If a header with the same name already exists in the request, the new *name:value* pair is added after the current *name:value* pair.

Example The following commands configure an SIP health monitor with hostname and customized header insertion.

```
ACOS(config)# health monitor sip_monitor
ACOS(config-health:monitor)# method sip hostname
a10networks.com
ACOS(config-health:monitor)# header-insert Expires:1800
```

NOTE: Space is also supported in the header content with a double quotation. For example, header-insert "Expires: 1800".

health external

Description File commands that create, edit, and manage external health monitor scripts.

Creating, editing, and deleting external health monitor scripts is only supported for administrative users provisioned with health monitor

(hm) privilege. If these operations fail due to insufficient privilege, contact your ACOS root administrator.

For more information and script examples, see the *Application Delivery Controller Guide* (*Using External Health Methods* section) and the *Management Access and Security Guide.*

Security Notes

- External health monitors run on a system-level basis at escalated privilege within the ACOS, independent of partition-level constraints.
- Creating or editing their underlying scripts represent an avenue for potentially malicious code to be introduced into the ACOS system which could be used to compromise security of the ACOS system or its connected environment.
- To better ensure confidentiality, integrity, and availability in an ACOS installation, external health monitor scripts should be carefully reviewed and audited to verify their contents are for the intended monitoring purpose and are free of unsanctioned or untrusted code.

Syntax

```
health external {
copy src-file dest-file |
create new-file [description] |
delete source |
edit source [description] |
rename source destination
```

Parameter	Description
copy src-file des-file	Copy the *src-file* script into the *dest-file* script.
create new-file [description]	Creates a script file and opens an editor to modify it.
delete src-file	Removes the *src-file*.
edit src-file [description]	Opens an editor to modify an existing script.
rename source destination	Rename an aFleX script from *src-name* to *dst-name*.

Mode Global configuration

Example This command creates an external health monitor script named hm-ex_1, adds a single line of code, then saves the file and exits the editor.

```
ACOS(config)# health external create hm-ex_1
Type in your Health External Script (type . on a line by
itself when done)
set an_connected -1
.
Done
ACOS(config)#
```

interval

Description Number of seconds between health check attempt, 1-180 seconds. A health check attempt consists of the ACOS device sending a packet to the server. The packet type and payload depend on the health monitor type. For example, an HTTP health monitor might send an HTTP GET request packet.

Syntax

```
[no] interval seconds [timeout  seconds]
```

Parameter	Description
interval *seconds*	Period between health check attempts, 1-180 seconds. Default is 5 seconds.
timeout *seconds*	Period that ACOS waits for a reply to a health check, 1-12 seconds. The default is 5 seconds.

Default See descriptions.

Mode Health monitor configuration

Example The following command is the configuration example:

```
ACOS(config)# health monitor test_monitor
ACOS(config-health:monitor)# interval 30 timeout 10
ACOS(config-health:monitor)#
```

method

Description Configure a health method.

Syntax

```
[no] method method-options
```

Valid parameters for *method-options* are shown in the following table:

Parameter	Description
compound sub *monitor-name* [**sub** *monitor-name* ...] *Boolean-operators*	Configures a compound health monitor. A compound health monitor consists of a set of health monitors joined in a Boolean expression (AND / OR / NOT). For more information, see the "Compound Health Monitors" section in the "Health Monitoring" chapter of the Application Delivery Controller Guide.
[**no**] **database** *database-type* **db-name** *name* **username** *username-string* **password** *password-string* [*query-options*]	Configures a database health monitor. The ACOS device sends a database query to the specified server. The following options can be configured:
	database *database-type* Specifies the type of database to test: • **mssql** • **mysql** • **oracle** • **postgresql**
	db-name *name* Specifies the name of the database to query.
	username *username-string* **password** *password-string* Specifies the login information required to access the database.
	query-options

Parameter	Description
	Specifies query information: **send** *query* [**receive** *expected-reply* | **receive-integer** *integer*][**row** *row-num* **column** *col-num*]
	send *query* SQL query to send to the database.
	receive *expected-reply* Query result expected from the database in order to pass the health check. To use the **receive** (1-31 characters) or **receive-integer** (0-2147483647) options, you also must use the **send** option. If you do not use **send**, the ACOS device does not send a query.
	row *row-num* **column** *col-num* For replies that consist of multiple results, the results are in a table. You can specify the row and column location within the results table to use as the receive string. If you do not specify the row and column, row 1 and column 1 are queried by default.
dns {**ipaddress** | **domain** *domain-name*} [*options*]	Sends a lookup request to the specified port number for the specified domain name. You can specify a **domain**name or a server **ipaddress** as the target of the health check. The following options can be configured:
	expect {response-code *code-list*|**ipv4-addr***ipv4 address* **| ipv6-addr** *ipv6 address*| **FQDN** *fqdn* Specifies the domain name or IP address expectation function for DNS method. You can

Parameter	Description
	configure the following expect. • **response-code***code-list*- Specify the list of response codes, in the range 0-15, that are valid responses to a health check. The DNS server can respond with any of the expected response codes. By default, the expect list is empty, in which case the ACOS device expects status code 0 (No error condition). • **ipv4-addr***<ipv4 address>* - Specify the IPv4 address expect. This expect can only be specified with type A. • **ipv6-addr***<ipv6 address>* - Specify the IPv6 address expect. This expect can only be specified with type AAAA. • **FQDN** *fqdn* - Specify the fully qualified domain name. This expect can only be specified with type CNAME, PTR and MX. The FQDN length can be between 1-255. Only alphabet, digit, hyphen, and period are allowed. Each label first and last character must be digit or letter, max length of each label is 63.
	domain For health checks sent to a domain name, specify the record type the responding server is expected to send in reply to health checks. You can specify one of the following record types: **type** {**A** | **CNAME** | **SOA** | **PTR** | **MX** | **TXT** | **AAAA**} – • A – IPv4 address record

Parameter	Description
	• CNAME – Canonical name record for a DNS alias • SNI - SNI specifies the hostname to client connection. • SOA – Start of authority record • PTR – Pointer record for a domain name • MX – Mail Exchanger record • TXT – Text string • AAAA – IPv6 address record By default, the ACOS device expects the DNS server to respond to the health check with an A record.
externalprogram *program-name* [**arguments** *argument-string* |**port** *portnum* |**root-shell** |**preference**]	Runs an external program (for example, a Tcl script) and bases the health status on the outcome of the program. See “Usage” below for more information on health check using an external program. The arguments option specifies arguments to pass tothe external application or script. The port option specifies the server port number toassociate with this health check. The root-shell option executes the external programin a root shell environment. Elevated privileges arerequired to access ACOS resources. For moreinformation on Privilege Shell Root license, referGlobal License Manager User Guide.

Parameter	Description
	NOTE: An additional Privilege Shell Root licenseis required to allow the execution of external programsusing the root-shell option. ACOS will not display theroot-shell option without this license. The **preference** option applies to weighted load-balancing methods such as SNMP-based load balancing. (See the "SNMP-based Load Balancing" chapter in the Application Delivery Controller Guide.) External health methods are not supported in Direct Server Return (DSR) deployments.
ftp [[**username** *name* **password** *string*] **port** *port-num*]	Sends an FTP login request to the specified port. Expects OK message, or Password message followed by OK message. Unless you use anonymous login, the username and password must be specified in the health check configuration.
http [*options*]	Sends an HTTP request to the specified TCP port and URL. Expects OK message (200). The following options can be configured:
	expect {**response-code** *code-list* | **response-code-regex** *regex-code-list* | *text-string* | **text-regex** *regex-text-string*} Specifies a response code, response code with regular expressions, a text string, or text string with regular expression expected from the server. To specify a range of response codes for **response-code**, use a dash (-) between the

Parameter	Description
	low and high numbers of the range. Use commas to delimit individual code numbers or separate ranges. By default, the ACOS device expects response code 200 (OK).
	host {*ipv4-addr* | *ipv6-addr* | *domain-name*} [:*port-num*] Replaces the information in the Host field of the request sent to the real server. By default, the real server's IP address is placed in the field.
	Kerberos-auth realm *realm_name* **kdc** *ip/ipv6-addr***port num** Specifies Kerberos authentication by using the HTTP negotiation mechanism. To enable Kerberos authentication on the health monitor, enter a Kerberos realm as well as the IP address of the KDC server and its related port.
	maintenance-code *code-list* Specifies a response code that indicates the server needs to be placed into maintenance mode. If the ACOS device receives the specified status code in response to a health check, the ACOS device changes the server's health status to Maintenance. When a server's health status is Maintenance, the server will accept new requests on existing cookie-persistent or source-IP persistent connections, but will not accept any other requests. To leave maintenance mode, the server must

Parameter	Description
	do one of the following: • Successfully reply to a health check by sending the expected string or response code, but without including the maintenance code. In this case, the server's health status changes to Up. • Fail a health check. In this case, the server's status changes to Down. The Maintenance health status applies to server ports and service-group members. When a port's status changes to Maintenance, this change applies to all service-group members that use the port. **NOTE:** The **expect maintenance-code** option applies only to servers in cookie-persistence or source-IP persistence configurations, and can be used only for HTTP and HTTPS ports.
	port *port-num* Specifies the protocol port on which the server listens for HTTP traffic. Use this option if the server does not use the default HTTP port, 80.
	url *string* Specifies the request type and the page (url-path) to which to send the request. By default, GET requests are sent for " / ", the index.html page. You can specify one of the following: • **GET** *url-path*

Parameter	Description
	• **HEAD** *url-path* • **POST** *url-path* **postdata** *string* • **POST / postfile** *filename* In a **postdata** string, use "=" between a field name and the value you are posting to it. If you post to multiple fields, use "&" between the fields. For example: **postdata** *fieldname1*=*value*&*fieldname1*=*value*. The string can be up to 255 bytes long.
	username *name* Specifies the username required for HTTP access to the server. Unless anonymous login is used, this option must be specified.
	version2 Configure this command to specify HTTP version2. **NOTE:** For this http option in ACOS, do not use the **partition shared** option from L3V.
https [*options*]	This option is similar to an HTTP health check, except SSL is used to secure the connection. The default port is 443. The following options are available to configure:
	cert *cert-name* and **key** *key-name* Add an SSL certificate and key to an HTTPS health monitor. When you use this option, the ACOS device uses the certificate and key during the SSL handshake with the HTTPS port on the

Parameter	Description
	server. The certificate you plan to use with the health monitor must be present on the ACOS device before you configure the health monitor.
	disable-sslv2hello Disables encapsulation of SSLv3, TLSv1, or TLSv1.1 hello messages within the SSLv2 hello messages for HTTPS health checks.
	expect-cert-name <*cert_name***>** Validates the certificate common name in the Server HELLO returns from the server. The host name string can have a length of up to 63 characters. The expected server certificate parameter specifies the common name of the SSL certificate.
	sni host <*host_name***>** Indicate SNI host and health monitor and requests a certificate for server name.

	http-version2
	
	Configure this command to specify HTTP/2 for HTTPS.
	
	To select the cipher list for the SSL handshake, apply the health monitor to the to the server-SSL health monitoring template, as described in the following example:
	
	`ACOS(config)#health monitor https`
	`ACOS(config-health:monitor)#server-ssl hm-server-ssl`

Parameter	Description
	`ACOS(config-health:monitor)#method https http-version2` **NOTE:** For this http option in ACOS, do not use the **partition shared** option from L3V.
imap [**port** *port-num*] [**username** *name* **password** *string* [**auth** *auth-type*]]	Sends an IMAP login request with the specified username *name* and password *string*. Expects reply with OK message. For the *auth-type*, you can specify one or more of the following authentication methods: • **cram-md5**—Challenge-response authentication. Note that the user's password will be used as the shared secret. • **login**—Simple login authentication. • **plain**—Plain text authentication. • If all three options are specified, **plain** will be selected. • If **plain** is not specified, then **cram-md5** will be used.
kerberos-kdc kinit *principal password* {*kdc-hostname* | *kdc-ipaddr*} [**port** *port-num*] [**tcp-only**]	Configures a method to check accessibility of the KDC for obtaining a TGT. • *principal* – Name of the Kerberos principal. This is the ACOS client name presented to the server. • *password* – Kerberos admin password. • {*kdc-hostname* | *kdc-ipaddr*} [**port** *port-num*] – Hostname or IP address of the server where the KDC is running. The **port** option specifies the protocol port on which the

Parameter	Description
	server listens for TGT requests. The default KDC port is 88. • **tcp-only** – Sends health checks only over TCP.
kerberos-kdc kadmin *realm-name principal password* {*kdc-hostname* | *kdc-ipaddr*} [**port** *port-num*] {admin-hostname | admin-ipaddr} [port port-num]	Configures a method to check accessibility of the Kerberos server for user account administration. • *realm-name* – Name of the Kerberos realm. • *principal* – Name of the Kerberos principal. • *password* – Kerberos admin password. • {*kdc-hostname* | *kdc-ipaddr*} [**port** *port-num*] – Hostname or IP address of the Kerberos server. The **port** option specifies the TCP port on which the server listens for user account administration requests. The default TCP port is 749. For information about the other options, see the descriptions for **kerberos-kdc kinit** (described above).
kerberos-kdc kpasswd principal password {kdc-hostname | kdc-ipaddr} [port port-num] {pwd-hostname | pwd-ipaddr} [port port-num]	Configures a method to check accessibility of the Kerberos server for user password change. • {*pwd-hostname* | *pwd-ipaddr*} [**port** *port-num*] – Hostname or IP address of the Kerberos server. The **port** option specifies the UDP port on which the server listens for user password-change requests. The default UDP port is UDP port 464. For information about the other options, see the descriptions for **kerberos-kdc kinit** (described above).

Parameter	Description
ldap [**StartTLS**] [**binddn** *dn-string password*] [**overssl**] [**port***port-num*] [**run-search***options*]	Configures a method to check accessibility the KDC for obtaining a TGT. • **StartTLS** – Begins the health check by sending a StartTLS request. • **binddn** *dn-string password* – DN name and password. • **overssl**– Uses TLS to secure the connection. • **port** *port-num*– UDP port on which the server listens for user password-change requests. The default UDP port is UDP port 464. • **run-search** *options* – Performs the specified database search. The following options are supported: • **BaseDN** *dn-string*– Searched the database for the specified DN. • **query** *query-string* [**AcceptNotFound**] – Sends the specified query string to the server. The **AcceptNotFound** option allows the health check to pass even if the search query is unsuccessful.
ntp	Sends an NTP client message to UDP port 123. Expects a standard NTP 48-byte reply packet.
pop3 **port***port-num* **username***name* **password***string*	Sends a POP3 user login request with the specified username and password. Expects reply with OK message.
radius username *name* **password***string*	Sends a Password Authentication Protocol (PAP) request to the specified port to authenticate the specified username. Expects

Parameter	Description
secret *string* **[port***port-num]* *[expectresponse-code code-list]*	Access Accepted message (reply code 2). The **secret** option specifies the shared secret required by the RADIUS server. The *code-list* can contain one or more numeric response codes. To specify more than one code, use commas but no spaces. (See "CLI Example" below.)
rtsp **port** *port-num* **rtspurl** *string*	Sends a request to the specified port for information about the file specified by **rtspurl**. Expects reply with information about the specified file.
sip [**register**] [**port** port-num] [**expect-response-code**] [**hostname**] [**tcp**]	Sends a SIP request to the SIP port. Expects 200 OK in response by default. • **expect-response-code** - This option specifies a set of SIP status codes. In this case, a SIP health check is successful only if the server reply includes one of the specified SIP status codes. You can specify **any** or a combination of individual code numbers and code ranges. Use commas as delimiters, with no spaces. Use a dash and no spaces to delimit the lower and upper values of a range. Examples: ◦ **expect-response-code 100,101,121,200** ◦ **expect-response-code 100-121,200** ◦ **expect-response-code any** • **hostname** - This option sends the SIP hostname (instead of IP address) that is used in the SIP request header for health monitoring. • **register** - This option to send a REGISTER

Parameter	Description
	request instead of the default OPTION request. • **tcp** - This option configures the health method for SIP over TCP/TLS. Without this option, the health method is for SIP over UDP.
smtp **domain** *domain-name* **port** *port-num* [**mail-from** *sender* **rcpt-to** *receiver*] [**starttls**]	Sends an SMTP Hello message to the specified server in the specified domain. Expects reply with OK message (reply code 250). An SMTP message is generated after establishing a TCP connection with the server. The message is sent only after the ACOS device sends the "HELO" message and receives the expected response. Use the **mail-from** option to specify the SMTP sender of this message, and the **rcpt-to** option to specify the recipient of this message. You can optionally specify a specific port number, and also check for STARTTLS support when the Hello message is received.
snmp [**port***port-num*] [**community***string*] [**oid***oid-name*] [**operation** {**get**|**getnext**}]	Sends an SNMP Get or Get Next request to the specified OID, from the specified community. Expects reply with the value of the OID. The OID can be **sysDescr**, **sysUpTime**, **sysName**, or another name in ASN.1 style. Although you can enter these objects in ASN.1 format, only MIB-2 OIDs are supported.
tacplus **username***username* **password***password* **secret***shared-secret*	Configures a method to check server availability by passing the TACACS+ parameters, with secret and password encrypted.If authentication is correct, a success message is returned that keeps the

Parameter	Description
[**port***portnum*] [**type inbound-ascii-login**]	server status marked as up. • *username* – Specify the username to authenticate (1-31 characters). • *password* – Specify the password to authenticate (0-31 characters). A password of '' means no password. • *shared-secret* – Specify the shared secret for the TACACS+ server (1-31 characters). • *port-num* – Specify the TACACS+ port (1-65534, default 49). • **type inbound-ascii-login** –The TACACS+ type. The currently supported type is inbound-ascii-login, which is also the default.
tcp port*port-num* [**halfopen**] [**send** *send-string* **response contains** *response-string*]	Sends a connection request (TCP SYN) to the specified TCP port on the server. Expects TCP SYN ACK in reply. By default, ACOS responds to the SYN ACK by sending an ACK. To configure ACOS to send a RST (Reset) instead, use the **halfopen** option. Use the **send** and **response contains** options to send and receive text strings in TCP health checks. The send-string is the string the ACOS device sends to the TCP port after the three-way handshake is completed. The response-string is the string that must be present in the server reply. Each string can be 1-127 characters long. If a string contain blank spaces or other special characters (for example, " / " or " \ "), use

Parameter	Description
	double quotation marks around the entire string.
udp port *port-num* [force-up-with-single-healthcheck]	Sends a packet with a valid UDP header and a garbage payload to the specified UDP port on the server. Expects either of the following: • server reply from the specified UDP port, with any type of packet. • server does not reply at all. The server fails the health check only if the server replies with an ICMP Error message. By default, the server is reported as UP after four health check packets are sent without a response. The force-up-with-single-healthcheck option programs the monitor to reports a server as UP after one health check packet.

Default The configuration has a default “ping” health monitor that uses the **icmp** method. The ACOS device applies the ping monitor by default. The ACOS device also applies the TCP or UDP health monitor by default, depending on the port type. These default monitors are used even if you also apply configured monitors to a service port.

To use differently configured ping or TCP/UDP monitors, configure new monitors with the ICMP, TCP, or UDP method and apply those monitors instead.

When specifying a protocol port number, specify the port number on the real server, not the port number of the virtual port. By default, the well-known port number for the service type of the health monitor is used. For example, for LDAP, the default port is 389 (or 636 if the **overssl** option is used).

If you specify the protocol port number in the health monitor, the protocol port number configured in the health monitor is used if you send an on-demand health check to a server without specifying the

protocol port. (See the “health-test” command in the Command Line Interface Reference. After you bind the health monitor to a real server port, health checks using the monitor are addressed to the real server port number instead of the port number specified in the health monitor’s configuration. In this case, you can override the IP address or port using the **override** commands described later in this chapter.

Mode Health monitor configuration

Usage To use a health method, you must do the following:

1. Configure a health monitor, by assigning a name to it and by assigning one of the health methods listed above to it. Use the **health monitor** command at the global Config level to create and name the monitor. (See the “health monitor” command in the Command Line Interface Reference.) Use the **method** command at the monitor configuration level to assign a health method to the monitor.
2. Apply the health monitor to a real server or real server port, using the **health-check** command at the configuration level for the server or the server port. Apply monitors that use the ICMP method to real servers. (See health-check.) Apply monitors that use any of the other types of methods to individual server ports. (See port.)
3. The **expect-cert-name** is an optional field. If configured, health monitor uses for the cert-name and **key-name** to validate the certificate Common Name (CN) received from Server. If it is not configured, health monitor uses user-defined SNI hostname (Server Name) as a default for
checking the certificate CN.

Example These commands apply health monitor “ping” to server “rs0”. The ping monitor is included in the ACOS device’s configuration by default and does not need to be configured.

```
ACOS(config)# slb server rs0 10.2.3.4
ACOS(config-real server)# health-check ping
```

Example The following commands configure health monitor “hm1” to use the TCP health method, and apply the monitor to a TCP port on real server “rs1”. The TCP health checks are sent to TCP port 23 on the server.

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method tcp port 23
ACOS(config-health:monitor)# exit
ACOS(config)# slb server rs1 1.1.1.1
ACOS(config-real server)# port 23 TCP
ACOS(config-real server-node port)# health-check hm1
```

Example The following commands configure health monitor “hm2” and set it to use the HTTP method. The health monitor is applied to port 80 on real server “rs1”.

```
ACOS(config)# health monitor hm2
ACOS(config-health:monitor)# method http
ACOS(config-health:monitor)# exit
ACOS(config)# slb server rs1 2.2.2.2
ACOS(config-real server)# port 80 http
ACOS(config-real server-node port)# health-check hm2
```

Example These commands configure a TCP health monitor that sends an HTTP GET request to TCP port 80, and expects the string “200” to be present in the reply:

```
ACOS(config)# health monitor tcp-with-http-get
ACOS(config-health:monitor)# method tcp port 80 send "GET /
HTTP/1.1\r\nHost: 22.1.2.2\r\nUser-Agent: a10\r\nAccept:
*/*\r\n\r\n" response contains 200
```

This health monitor sends an HTTP GET request to TCP port 80 on the target server. This particular request uses the following header fields:

- Host – Specifies the host (server) to which the request is being sent.
- User-Agent – Identifies the entity (user agent) that is sending the request. In this example, the sending entity is “a10”.
- Accept – Specifies the types of media that are allowed in the response. This example uses wildcards (*/*) to indicate that any valid media type and range are acceptable.

If the string “200” is present anywhere in the reply from the port, the port passes the health check.

Example

The following commands configure a RADIUS health monitor that accepts response code 2 or 3 as passing (healthy) responses from a server:

```
ACOS(config)# health monitor rad1
ACOS(config-health:monitor)# method radius port 1812 expect
response-code 2,3 secret a10rad username admin1 password pwd1
```

Example

Here is an external health-check example. Besides internal health checks, which use a predefined health check method, you can use external health checks with any of the following types of scripts are supported:

- Perl
- Shell
- TCL

Utility commands such as ping, ping6, wget, dig, and so on are supported.

For Tcl scripts, the health check parameters are transmitted to the script through the predefined TCL array ax_env. The array variable ax_env(ServerHost) is the server IP address and ax_env(ServerPort) is the server port number. Set ax_env(Result) 0 as pass and set the others as fail. TCL script filenames must use the “.tcl” extension.

To use the external method, import the program onto the ACOS device. The script execution result indicates server status, which is stored in ax_env(Result).

The following commands import external program “ext.tcl” from FTP server 192.168.0.1, and configure external health method “hm3” to use the imported program to check the health of port 80 on the real server:

```
ACOS(config)# health external import "checking HTTP server"
ftp://192.168.0.1/ext.tcl
ACOS(config)# health monitor hm3
ACOS(config-health:monitor)# method external port 80 program
ext.tcl
```

```
SNI specifies the hostname to client connection.
ACOS(config-health:monitor)# method https sni host
a10networks.com expect-cert-name aa
```

For additional information and more examples, see the “External Health Method Examples” section in the “Health Monitoring” chapter of the Application Delivery Controller Guide.

Example The following commands configure a DNS health monitor that expect ipv4-addr as an answer for type A resolution from a server:

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method dns domain a10networks.com
expect ipv4-addr 10.2.1.12
```

Example The following commands configure a DNS health monitor that expect FQDN as an answer for IPv6 reverse resolution from a server.

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method dns ipaddress <ipv6
address> expect FQDN <fqdn>
```

override-ipv4

Description Send the health check to a specific IPv4 address, instead of sending the health check to the IP address of the real server or GSLB service IP to which the health monitor is bound. This command and the other override commands are particularly useful for testing the health of remote links.

Syntax

```
[no] override-ipv4  ipaddr
```

Default By default, a health check is addressed to the real server IP address of the server to which the health monitor is bound.

Mode Health monitor configuration

Example The following commands configure a health monitor to check 192.168.1.1:

```
ACOS(config)# health monitor site1-hm
ACOS(config-health:monitor)# method icmp
ACOS(config-health:monitor)# override-ipv4 192.168.1.1
```

override-ipv6

Description Send the health check to a specific IPv6 address, instead of sending the health check to the IP address of the real server to which the health monitor is bound.

Syntax

```
[no] override-ipv6  ipv6addr
```

Default By default, a health check is addressed to the real server IP address of the server to which the health monitor is bound.

Mode Health monitor configuration

Example These commands configure a health monitor to check 2001:db8::1521:31ab:

```
ACOS(config)# health monitor site2-hm
ACOS(config-health:monitor)# method icmp
ACOS(config-health:monitor)# override-ipv6 2001:db8::1521:31ab
```

override-port

Description Send the health check to a specific protocol port, instead of sending the health check to the server port to which the health monitor is bound.

Syntax

```
[no] override-port  portnum
```

Default By default, a health check is addressed to the protocol port number to which the health monitor is bound.

Mode Health monitor configuration

Example These commands configure a health monitor to check port 8081 on 192.168.1.1:

```
ACOS(config)# health monitor site3-hm
ACOS(config-health:monitor)# method http
ACOS(config-health:monitor)# override-ipv4 192.168.1.1
ACOS(config-health:monitor)# override-prt 8081
```

passive

Description Configures inband health monitoring based on HTTP status code.

Syntax

```
[no] passive
{status-code-2xx | status-code-non-5xx}
[passive-interval seconds]
[sample-threshold samples-per-second]
[threshold percent]
```

Parameter	Description
status-code-2xx | status-code-non-5xx	Healthy status code numbers – These status codes indicate the HTTP service is healthy. You can specify any 2xx status code or any status code *except* a 5xx code.
passive-interval *seconds*	The health-monitor interval that is used when passive health monitoring is activated. For proper operation of the feature, the passive interval should be longer than the health monitor's interval. You can specify 1-180 seconds. The default is 10 seconds.
sample-threshold *samples-per-second*	Minimum number of server replies that must contain one of the specified status codes, within a one-second interval, before passive health monitoring is enabled. The sample threshold prevents passive health monitoring from taking effect after only a small total number of samples are taken. You can specify 1-10000 samples per second. The default is 50.
threshold *percent*	Minimum percentage of server replies that must contain a healthy status code, within a given one-second interval, before passive health monitoring is activated. You can specify 0-100 percent. The default is 75 percent. If you specify 0, this parameter is disabled, in which case there is no minimum threshold.

Default See descriptions.

Mode Health monitor configuration

Example

The following commands create a new health monitor, and enable passive health-monitoring mode:

```
ACOS(config)# health monitor http-passive
ACOS(config-health:monitor)# passive status-code-2xx
ACOS(config-health:monitor)# method http
```

The following commands configure a real server, service group, and virtual server. The HTTP health monitor configured above is applied to the TCP port on the real server.

```
ACOS(config)# slb server ser1 172.168.1.107
ACOS(config-real server)# no health-check
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# health-check http-passive
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg1 tcp
ACOS(config-slb svc group)# member ser1 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb virtual-server vs1 172.168.6.100
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# service-group sg1
```

proxy-header

Description

Configure this command for health check with HA (High Availability) proxy header.

Using the HA proxy protocol, the connection information such as a client's address can be communicated safely across multiple layers of NAT or TCP proxies. At the beginning of each connection, the connection initiator places an easily parsable header.

Syntax

```
[no] proxy-header {v1| v2}
```

Parameter	Description
v1	The outcome of version 1 is in human readable header format. This is useful while debugging.

Parameter	Description
v2	Version 2 supports binary encoding of a header which makes it easy to parse.

Default Disabled

Mode Health monitor configuration

Usage Using this command, v1 or v2 can be specified for the proxy-header format.

Health checks using proxy header format are supported only for method types TCP, HTTP and HTTPS. If the proxy header is enabled for the method types other than TCP, HTTP and HTTPS, an error message is displayed.

Example The following example enables **proxy-header v1** for health monitor hm:

```
ACOS (config) #health monitor hm
ACOS (config-health:monitor) #method http
ACOS (config-health:monitor) #proxy-header v1
```

Example The following example displays an error message when the method type is changed to icmp after the **proxy-header v1** is enabled as shown in the example given above:

```
ACOS (config) #health monitor hm
ACOS (config-health:monitor) #method http
ACOS (config-health:monitor) #proxy-header v1
ACOS (config-health:monitor) #method icmp
Proxy header is configured but only supports method types
tcp/http/https.
```

In this case, the method icmp is applied, but the proxy protocol does not perform any operation:

```
ACOS (config-health:monitor) #sh context
!Context configuration: 40 bytes
!
health monitor hm
 proxy-header v1
!
```

Example The following example displays an error message while trying to enable **proxy-header v1** for health monitor hm1 with method snmp:

```
ACOS (config) #health monitor hm1
ACOS (config-health:monitor) #method snmp
ACOS (config-health:monitor) #proxy-header v1
Proxy header is not supported on configured method.
```

In this case, the method snmp is applied, but the proxy protocol is not enabled:

```
ACOS (config-health:monitor) #sh context
!Context configuration: 37 bytes
!
health monitor hm1
 method snmp
!
```

NOTE: This feature is applicable only to the health checks that establish connection on L4 protocols.

retry

Description Maximum number of times ACOS will send the same health check to an unresponsive server before determining that the server is down. You can specify 1-10.

Syntax

```
[no] retry number
```

Default 3

Mode Health monitor configuration

Example The following command is the configuration example:

```
ACOS(config)# health monitor test_monitor
ACOS(config-health:monitor)# retry 5
ACOS(config-health:monitor)#
```

server-ssl

Description Configures server-side SSL template for health monitoring on the data plane.

Syntax

```
[no] server-ssl name
```

Parameter	Description
name	Name of the server-side SSL template. The length can be 1 -127 characters.

Default NA

Mode Health monitor configuration

Usage ACOS supports SSL-based health monitoring on the data plane. The health monitor could utilize SSL acceleration hardware and allow ACOS data plane processes to manage HTTPS connections directly.

To enable this feature, you must create the server-SSL template and bind it to the data plane health monitor using this command. The following configurations are supported:

- Server SSL template configuration can include version, session-ticket-enable, and cipher settings.

For HTTP/3 health monitoring on the data plane, if you configure session-ticket-enable then you must also configure early-data setting.

- Health monitor method configuration can include **expect-cert-name**, **sni host**, **port**, **url**, **maintenance-code**, **http-version2**, **cert** and **key**, and **http-version3** settings and can be bound to a real port or service group

Example Bind the server SSL template to health monitoring and configure HTTPS method.

```
ACOS(config)# health monitor hm-dplane-https
ACOS(config-health:monitor)# server-ssl hm-server-ssl
ACOS(config-health:monitor)# method https http-version2
```

Related Commands:

- slb template server-ssl
- slb template cipher
- method

ssl-ciphers

Description Specify the ciphers to use in the health check of a real server or real server port.

Syntax

```
[no] ssl-ciphers openSSL-ciphers
```

Parameter	Description
openSSL-ciphers	The OpenSSL Project `ciphers` command. For information on the OpenSSL Project `ciphers` command, see the ciphers manpage in the OpenSSL Project documentation.

Mode Health monitor configuration

Example Configure a health monitor to use the default OpenSSL Project cipher suite with the exclusion of EDH ciphers.

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-ciphers DEFAULT:!EDH
ACOS(config-health:monitor)# method https
```

Example Bind the `hm-https` health monitor to the **s1** real server on its `1.1.1.1` network interface.

```
ACOS(config)# slb server s1 1.1.1.1
ACOS(config-real server)# health-check hm-https
ACOS(config-real server)# end
```

Example Bind the **hm-https** health monitor to the TCP port 80 of the **s1** real server on its `1.1.1.2` network interface. Also apply the **Server_SSL1** server-SSL template to the same port.

If the **Server_SSL1** server-SSL template specifies a cipher suite in its configuration (`cipher` command), that cipher suite takes precedence if and only if the ACOS Device is equipped with hardware that supports the cipher. The supported cipher are listed at:

https://www.a10networks.com/support/axseries.

```
ACOS(config)# slb server s1 1.1.1.2
ACOS(config-real server)# port 443 tcp
```

```
ACOS(config-real server-node port)# template server-ssl
Server_SSL1
ACOS(config-real server-node port)# health-check hm-https
ACOS(config-real server-node port)# end
```

ssl-ticket

Description Enable SSL ticket session resumption for HTTPS health monitor method.

Syntax

```
[no] ssl-ticket
```

Mode Health monitor configuration

Example The following command enables ssl-ticket for HTTPS health monitor method.

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-ticket
ACOS(config-health:monitor)# method https
```

ssl-ticket lifetime

Description Specify number of seconds the ticket will be valid from time of creation. Update the HTTPS method to leverage session ticket when doing SSL handshake.

Syntax

```
[no] ssl-ticket lifetime seconds
```

Parameter	Description
seconds	Specify the lifetime value in seconds. The value can be between 0-2147483647 seconds. If you set the lifetime to '0' then the feature will be disabled.

Mode Health monitor configuration

Example Configure a HTTPS health monitor to use ssl-ticket lifetime.

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-ticket lifetime 4120
ACOS(config-health:monitor)# method https
```

ssl-version

Description Specify the preferred SSL version to be used with HTTPS health monitor method for negotiation.

Syntax

```
[no] ssl-version {31 | 32 | 33 | 34} {31 | 32 | 33 | 34}
```

Parameter	Description
31	SSL/TLS v1.0.
32	SSL/TLS v1.1.
33	SSL/TLS v1.2.
34	SSL/TLS v1.3.

Default Not enabled.

Mode Health monitor configuration mode

Usage The first ssl-version number is the preferred SSL version and the second ssl-version number is for downgrading the SSL version.

- If you want to downgrade the SSL version, then specify the minimum SSL version to which a session can be downgraded. For example, **ssl-version 34 31**.
- If you want to disable downgrading, then specify the same SSL-version number for both. For example, **ssl-version 34 34**.

Example Example configuration:

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-version 34 34
ACOS(config-health:monitor)# method https
```

strictly-retry-on-server-error-response

Description Force the ACOS device to wait until all retries are unsuccessful before marking a server or port Down.

Syntax

```
[no] strictly-retry-on-server-error-response
```

Default Disabled. For some health method types, the ACOS device marks the server or port Down after the first failed health check attempt, even if the retries option for the health monitor is set to higher than 0.

Mode Health monitor configuration

Usage This command applies to all types of health monitors. However, if you use an HTTP health monitor.that expects a string in the server reply and the string is missing, the port on the ACOS device is marked as down. By default, if the server's HTTP port does not reply to the first health check attempt with the expected string, the ACOS device immediately marks the port Down.

Example The following commands configure an HTTP health monitor that checks for the presence of "testpage.html", and enable strict retries for the monitor.

```
ACOS(config)# health monitor http-exhaust
ACOS(config-health:monitor)# method http url GET
/testpage.html
ACOS(config-health:monitor)# strictly-retry-on-server-error-
response
```

up-retry

Description Number of consecutive times the ACOS device must pass the same periodic health check, in order to be marked Up. You can specify 1-63.

Syntax

```
[no] up-retry number
```

Default 1

Mode Health monitor configuration

Example The following command is the configuration example:

```
ACOS(config)# health monitor test_monitor
ACOS(config-health:monitor)# up-retry 3
ACOS(config-health:monitor)#
```

slb common

Description Access the SLB configuration level for system-wide SLB parameters.

Syntax

```
slb common
```

NOTE: Commands in SLB common configuration mode are only available in the shared partition.

Mode Configuration mode

aflex-table-entry-aging-interval

Description Configure aFlex table entry aging interval in seconds. These aFlex tables will be synchronized with ACOS device via VRRP-A.

Syntax

```
[no] aflex-table-entry-aging-interval <1-3600>
```

Default Disabled

Mode SLB common configuration mode

Example This following command configures aFlex table entry parameters.

```
ACOS(config)# slb common
ACOS(config-common)# aflex-table-entry-aging-interval 3000
```

NOTE: For detailed information about aFlex tables and VRRP-A commands, refer *aFleX Scripting Language Reference* and *Configuring VRRP-A High Availability* guides.

aflex-table-entry-sync

Description Configure aFlex table entry parameters. These aFlex tables will be synchronized with ACOS device via VRRP-A.

Syntax

```
[no] aflex-table-entry-sync {max-key-len | max-value-len |
min-lifetime}
```

Parameter	Description
max-key-len	Specify the aFlex table entry maximum key length to synchronize. The value can be between 0-1000. '0' means that the key length shall not be used as a metrics to decide if the sync should happen or not.
max-value-len	Specify the aFlex table entry maximum value length to synchronize. The value can be between 0-1000. '0' means that the key length shall not be used as a metrics to decide if the sync should happen or not.
min-lifetime	Specifies the aFlex table entry minimum lifetime to synchronize. The value can be between 0-65535. '0' means that the lifetime shall not be used as a metrics to decide if the sync should happen or not.

Default Disabled

Mode SLB common configuration mode

Usage ACOS supports aFlex table synchronization in the VRRP-A cluster. This will help you to synchronize and recover aFlex when ACOS is rebooted.

The aFlex message is sent to the ACOS device using the key length, value length, table name as well as some other parameters. If the sum of this is less than 1000 then the data is sent to the ACOS standby device.

Example This following command configures aFlex table entry parameters.

```
ACOS(config)# slb common
ACOS(config-common)# aflex-table-entry-sync
ACOS(config-common-aflex-table-entry-sync)#max-key-len 50
ACOS(config-common-aflex-table-entry-sync)#max-value-len 100
ACOS(config-common-aflex-table-entry-sync)#min-lifetime 3600
```

NOTE: For detailed information about aFlex tables and VRRP-A commands, refer *aFleX Scripting Language Reference* and *Configuring VRRP-A High Availability* guides.

ecmp-hash

Description The option allows hashing on connection information (source IP, source port, destination port from forward tuple and real server IP), which would allow a more balanced (Equal-cost multi-path routing) protocol routing.

For IP based protocols, source IP and real server IP will be used for hashing. IPv4 to IPv6 or IPv6 to IPv4 routing is not supported.

Syntax

```
[no] ecmp-hash {system-default | connection-based}
```

Parameter	Description
system-default	Uses system default ecmp hashing algorithm.
connection-based	Uses connection information for hashing.

Mode SLB common configuration mode

Example The example mentioned below shows how to enable connection-based hashing:

```
ACOS(config)# slb common
ACOS(config-common)# ecmp-hash connection-based
```

NOTE: SSLi_L2 is not supported and smart nat is partially supported.

low-latency

Description Enables low latency mode. The system needs to be rebooted after configuring this option.

Limitation Following are the limitations of this command:

- Basic TCP and FIX IPv4 traffic supported.
- Physical platforms with TCAM hardware supported.
- Only applicable for shared partition.

Syntax `[no] low-latency`

Default Disabled

Mode SLB common configuration mode

Example The following command sets the low-latency:

```
ACOS(config)# slb common
ACOS(config-common)# low-latency
```

service-group-on-no-dest-nat-vports

Description Bind one service-group under multiple virtual-server when 'no-dest-nat' is enabled.

Limitation Health check operating in DSR mode is incompatible if a user enables **dsr-health-check-enable** and binds same service-group on multiple **no-dest-nat** virtual ports.

Syntax `[no] service-group-on-no-dest-nat-vports [allow-same | enforce-different]`

Parameter	Description
allow-same	Allow the binding service-group on no-dest-nat virtual ports.
enforce-different	Enforce that the same service-group can not be bound on different **no-dest-nat** virtual ports. This configuration is supported in both shared and L3V partitions

Mode SLB Common

Usage In some cases, there may be a specific requirement where user must bind one service-group under multiple virtual-server with 'no-dest-nat' enabled.

Example The following example configures this command:

```
ACOS(config)# slb common
ACOS(config-common)# service-group-on-no-dest-nat-vports
allow-same
```

buff-thresh

Description Fine-tune thresholds for SLB buffer queues.

CAUTION: Do not use this command except under advisement from A10 Networks.

Syntax

```
[no] buff-thresh
hw-buff num
relieve-thresh num
sys-buff-low num
sys-buff-high num
```

Parameter	Description
hw-buff *num*	IO buffer threshold. For each CPU, if the number of queued entries in the IO buffer reaches this threshold, fast aging is enabled and no more IO buffer entries are allowed to be queued on the CPU's IO buffer.
relieve-thresh *num*	Threshold at which fast aging is disabled, to allow IO buffer entries to be queued again.
sys-buff-low *num*	Threshold of queued system buffer entries at which ACOS begins refusing new incoming connections.
sys-buff-high *num*	Threshold of queued system buffer entries at which the ACOS device drops a connection whenever a packet is received for that connection.

Default N/A

Mode SLB common configuration mode

cert-pinning

Description Configure the certificate pinning list settings. In this setting, you can set the Time-to-Live (TTL) entries in the candidate list.

Syntax

```
[no]cert-pinning {ttl {1-1008} | candidate-list-feedback-opt-in {enable | schedule | use-mgmt-port}
```

Parameter	Description
ttl	Specifies the TTL entries in the locally generated certificate pinning candidate list. The value can be between 1-1008 (multiples of 10 minutes). By default, the value is set to 144 i.e. 1440 minutes (one day).
candidate-list-feed-back-opt-in	Specify the opt-in to improve A10's certificate-pinning sites list. The following sub-commands are available:
enable	Enable the candidate list feedback option.
schedule	Specify the schedule for uploading the local cert pinning list to central list service. By default, the value is set to daily 00:00. The following options can be configured: • *daily* - Specify the daily time to update the feedback. The time is *hh:mm* 24-hours local time format. • *weekly* - Specify the weekly day and time to update the feedback. The week can be specified as: `Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday`. The time can be specified as 24-hours local time format.: `hh:mm`
use-mgmt-port	Specify the use management port to connect to the A10 server.

Default NA

Mode SLB common configuration mode

Example The following example configures the cert-pinning:

```
ACOS(config)# slb common
ACOS(config-common)# cert-pinning
ACOS(config-common-cert-pinning)# ttl 360
```

Example The following example configures the candidate list feedback option:

```
ACOS(config)# slb common
ACOS(config-common)# cert-pinning
ACOS(config-common-cert-pinning)# cert-pinning candidate-list-feedback-opt-in
ACOS(config-common-cert-pinning-candidate...)# enable
ACOS(config-common-cert-pinning-candidate...)# schedule weekly monday 00:00
ACOS(config-common-cert-pinning-candidate...)# use-mgmt-port
ACOS(config-common-cert-pinning-candidate...)# exit
```

Related Commands:

- forward-proxy-bypass local-cert-pin-list
- forward-proxy-bypass central-cert-pin-list

compress-block-size

Description Change the default compression block size used for SLB.

Syntax

```
[no] compress-block-size bytes
```

The *bytes* option specifies the default compression block size, 6000-32000 bytes.

Default 16000

Mode SLB common configuration mode

Example The following example sets the compression block size to 16000 bytes:

```
ACOS(config)# slb common
ACOS(config-common)# compress-block-size 16000
```

conn-rate-limit src-ip

Description Configure source-IP based connection rate limiting.

All connection requests in excess of the connection limit that are received from a client within the limit period are dropped. This action is enabled by default when you enable the feature, and can not be disabled.

NOTE: For configuring connection rate limits on IPv6 traffic, use class lists. For more information, see "class-list" in the *Command Line Interface Reference* and "Understanding Class Lists" in the *DDoS Mitigation Guide for ADC*.

Syntax

```
[no] conn-rate-limit src-ip {tcp | udp} conn-limitper {100 | 1000}
[shared] [exceed-action [log] [lock-out lockout-period]]
```

Parameter	Description
tcp | **udp**	Specifies the Layer 4 protocol for which the filter applies.
conn-limit	Specifies the connection limit. The connection limit is the maximum number of connection requests allowed from a client, within the limit period. You can specify 1-1000000 (one million).
per {**100** | **1000**}	Specifies the limit period, The limit period is the interval to which the connection limit is applied. A client is conforming to the rate limit if the number of new connection requests within the limit period does not exceed the connection limit. You can specify 100 milliseconds or 1000 milliseconds.
shared	Specifies that the connection limit applies in aggregate to all virtual ports. If you omit this option, the limit applies separately to each virtual port.
exceed-action	Enables optional exceed actions: • **log** - Enables logging. Logging generates a log message when a client exceeds the connection limit.

Parameter	Description
	• **lock-out***lockout-period* - Locks out the client for a specified number of seconds. During the lockout period, all connection requests from the client are dropped. The lockout period can be 1-3600 seconds (1 hour). There is no default.

Mode SLB common configuration mode

Example The following commands allow up to 1000 connection requests per one-second interval from any individual client. If a client sends more than 1000 requests within a given limit period, the client is locked out for 3 seconds. The limit applies separately to each individual virtual port. Logging is not enabled.

```
ACOS(config)# slb common
ACOS(config-common)# conn-rate-limit src-ip tcp 1000 per 1000
exceed-action lock-out 3
```

Example The following commands allow up to 2000 connection requests per 100-millisecond interval. The limit applies to all virtual ports together. Logging is enabled but lockout is not enabled.

```
ACOS(config)# slb common
ACOS(config-common)# conn-rate-limit src-ip tcp 2000 per 100
shared exceed-action log
```

Example These commands allow up to 2000 connection requests per 100-millisecond interval. The limit applies to all virtual ports together. Logging is enabled and lockout is enabled. If a client sends more than 2000 requests within a given limit period, to one or more virtual ports, the client is locked out for 3 seconds.

```
ACOS(config)# slb common
ACOS(config-common)# conn-rate-limit src-ip tcp 2000 per 100
shared exceed-action log lock-out 3
```

ddos-protection

Description Enables hardware blocking of VIP traffic that is addressed to an unconfigured virtual port.

Syntax `ddos-protection {enable | disable}`

Parameter	Description
enable | **disable**	Enables or disables hardware blocking of VIP traffic. Default value is `disable`.

Default disabled

Mode SLB common configuration mode

Example This example enables hardware blocking of traffic to unconfigured virutal ports.

```
ACOS(config)# slb common
ACOS(config-common)# ddos-protection enable
```

ddos-protection logging

Description Enables logging of VIP traffic hardware blocking events.

Syntax `ddos-protection logging {enable | disable}`

Parameter	Description
enable | **disable**	Enables or disables hardware blocking. Default value is **enable.**

Default enabled

Mode SLB common configuration mode

Example This example disables the logging of hardware blocking of traffic to unconfigured virutal ports.

```
ACOS(config)# slb common
ACOS(config-common)# ddos-protection logging disable
```

ddos-protection packets-per-second

Description Enables logging of VIP traffic hardware blocking events.

Syntax `ddos-protection packets-per-second {tcp | udp} packet-rate`

Parameter	Description
tcp | udp	Specifies the data type of traffic affected by command.
packet-rate	Specifies data rate on virtual port that triggers hardware blocking. Value ranges from 0 to 65535. Default value is 200.

Default 200 packets per second for TCP or UDP traffic

Mode SLB common configuration mode

Example This example sets the device to begin hardward blocking for any unconfigured TCP ports that exceed 1000 packets per second.

```
ACOS(config)# slb common
ACOS(config-common)# ddos-protection enable
ACOS(config-common)# ddos-protection packets-per-second tcp
1000
```

disable-adaptive-resource-check

Description In cases where data packets smaller than a pre-configured size limit are received, HTTP sessions may be deleted when the number of such packets received exceeds a pre-defined threshold. This is the default behavior on an ACOS device.

The **disable-adaptive-resource-check** command disables the default behavior.

Syntax

```
[no] disable-adaptive-resource-check
```

Default Adaptive resource checking is enabled by default.

Mode SLB common configuration mode

disable-persist-scoring

Description Disables persist scoring method globally. The command can be used to disable regular scoring system for server selection and enable server selection based on the configuration of the service groups.

Syntax

```
[no] disable-persist-scoring
```

Mode SLB common configuration mode

Example Disable persist scoring:

```
ACOS(config)# slb common
ACOS(config-common)# disable-persist-scoring
```

disable-server-auto-reselect

Description Stop the ACOS device from automatically reselecting a lower priority server until a server with a higher priority is marked as Down or Disabled.

This is commonly used with inband health monitors.

Syntax

```
[no] disable-server-auto-reselect
```

Default Server auto-reselection is enabled by default.

Mode SLB common configuration mode

Usage When server priority is configured, the ACOS device sends all traffic to the highest priority server, until that server starts responding slowly or meets other negative conditions. This feature stops the ACOS device from automatically reselecting a lower priority server until a server with a higher priority is marked as Down or Disabled.

When a Data CPU reaches 70%, **slb disable-server-auto-reselect** will automatically activate and can be seen in the running config. When the Data CPU goes back down below 50% it will remove itself.

Example Enable the feature.

```
ACOS(config)# slb common
ACOS(config-common)# disable-server-auto-reselect
```

dns-cache-age

Description Configure the amount of time the ACOS device locally caches DNS replies.

DNS cache aging is applicable only when DNS caching is enabled, using the dns-cache-enable command. A DNS reply begins aging as soon as it

is cached and continues aging even if the cached reply is used after aging starts. Use of a cached reply does not reset the age of that reply.

Server response TTL is the minimum TTL of all resource records in that response. The honor-server-response-ttl command enables using TTL in the server response as DNS cache TTL.

Syntax `[no] dns-cache-age seconds`

Default 300

Mode SLB common configuration mode

The DNS cache TTL is calculated as follows:

1. If only the TTL is specified, then the specified TTL is used as DNS cache TTL.
2. If only the **honor-server-response-ttl** is enabled, then the TTL in server response is used as DNS cache TTL.
3. If the TTL is specified and **honor-server-response-ttl** is enabled, the minimum TTL between the specified TTL and server response TTL is used as DNS cache TTL.
4. If the TTL is not specified and **honor-server-response-ttl** is not enabled, the default value (300 seconds) will be used as DNS cache TTL.

Example This example configures the ACOS device to cache DNS replies for 300 seconds.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-age 300
```

Example This example configures the age of global DNS cache to be the minimum value between 600 seconds and the server response TTL:

```
ACOS(config-common)# dns-cache-age 600
ACOS(config-common)# honor-server-response-ttl
```

Example This example configures the age of the global DNS cache to be 600 seconds:

```
ACOS(config-common)# dns-cache-age 600
```

Example This command configures the server response TTL to be used as the global DNS cache TTL:

```
ACOS(config-common)# dns-cache-age
ACOS(config-common)# honor-server-response-ttl
```

dns-cache-age-min-threshold

Description Configures minimum age threshold for DNS cache entry.

Syntax

```
[no] dns-cache-age-min-threshold seconds
```

Configure a value between 1 to 1000000 seconds.

Default 0 seconds

Mode SLB common configuration mode

Usage DNS cache aging is applicable only when DNS caching is enabled using the dns-cache-enable command. The value is set to the specified entry instead of the default minimum DNS cache threshold value.

Example This example configures minimum age threshold to 155 seconds.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-enable
ACOS(config-common)# dns-cache-age-min-threshold 155
ACOS(config-common)# dns-cache-entry-size 1300
ACOS(config-common)# honor-server-response-ttl
```

Check the TTL value as mentioned below:

```
ACOS(config-common)# show dns cache entry
                                        S = DNSSEC, T = Type,
C = Class, W = weight
                                        Qlen = Query length,
Rlen = Response length
Domain                  S   T   C   Qlen  Rlen  TTL    Age
W  Hit
-----------------------------------+---+---+-----+-----+------
-+----
Global Table
www.finalanswer.com     0   1   1   37    222   155     0
1  0
```

```
Total: 1
```

dns-cache-aging-weight

Description Sets DNS cache entry weight.

Syntax

```
[no] dns-cache-aging-weight <num>
```

Replace *<num>* with a value between 1 to 7.

Default 1

Mode SLB common configuration mode

Usage The setting applies to the global DNS cache table. The specified weight deletes the entries as mentioned below:

- If the cache is more than 60% full, entries with weight 1 are eligible to be deleted.
- If the cache is more than 70% full, entries with weight 1-2 are eligible to be deleted.
- If the cache is more than 80% full, entries with weights 1-4 are eligible to be deleted.
- If the cache is more than 90% full, entries with weights 1-6 are eligible to be deleted.

Example The following example sets the DNS cache entry weight to 3:

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-enable
ACOS(config-common)# dns-cache-aging-weight 3
```

dns-cache-enable

Description Globally enable caching of replies to DNS queries.

Syntax

```
[no] dns-cache-enable
[
round-robin [ttl-threshold seconds] |
single-answer [ttl-threshold seconds] |
ttl-threshold seconds
]
```

Parameter	Description
round-robin	For DNS replies that contain multiple IP addresses in the ANSWER section, the ACOS device rotates the addresses when replying to client requests. The DNS transaction ID (which is random) is used to assist in the round-robin. This behavior is better for heavy traffic, but the side effect is that it will not strictly follow the round-robin.
single-answer	Caches only replies that have one IP address in the ANSWER section.
ttl-threshold *second*	Specifies the minimum Time-To-Live (TTL) a reply from the DNS server must have, in order for the ACOS device to cache the reply. You can specify 1-10000000 seconds.

Default DNS caching is disabled by default. Disabled. When you globally enable DNS caching, the **round-robin** and **single-answer** options are disabled by default. The default TTL threshold is 0 (unset).

Mode SLB common configuration mode

Usage When DNS caching is enabled, the ACOS device sends the first request for a given name (hostname, fully-qualified domain name, URL, and so on) to the DNS server. The ACOS device caches the reply from the DNS server, and sends the cached reply in response to the next request for the same name.

The ACOS device continues to use the cached DNS reply until the reply times out. After the reply times out, the ACOS device sends the next request for that URL to the DNS server, and caches the reply, and so on.

Enabling the single-answer option prevents the caching of DNS replies that have multiple IP addresses. For example, if a DNS response to a query for “www.example1.com” and the DNS reply has only one IP address (1.1.1.1), then the reply will be cached on the ACOS device. However, if the DNS response to a query for “www.example2.com” has two IP addresses (2.2.2.2 and 3.3.3.3), then the entry would not be cached on the ACOS device.

If the ttl-threshold option is configured on the ACOS device, then DNS replies will only be cached if they have a TTL value that is larger than the TTL threshold configured on the ACOS device. This prevents the ACOS device from caching DNS entries that will expire shortly thereafter.

For example, if the ACOS device's TTL threshold is set to 7200 seconds and the ACOS device receives a DNS response for a domain with a TTL of only 10 seconds, there would be little benefit in caching that DNS reply, since it will soon expire. Despite the cached information, subsequent client requests for that same domain would bypass the "stale" information cached on the ACOS device to perform another DNS lookup just 10 seconds later.

DNS caching applies to DNS requests sent to UDP as well as TCP virtual ports in a DNS SLB configuration.

Example The following example enables DNS caching on the ACOS device with all the default values.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-enable
```

dns-cache-entry-size

Description Set the maximum size in bytes for DNS cache entries.

Syntax

```
[no] dns-cache-entry-size num
```

Replace num with the desired DNS cache entry size, in bytes (1 - 4096).

Default 256

Mode SLB common configuration mode

Example The following example sets the DNS cache entry size to 3600 bytes:

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-entry-size 3600
```

dns-cache-sync

Description Enables high availability (HA) synchronization of global DNS cache entries.

Syntax

```
[no] dns-cache-sync
```

Default Disabled

Mode SLB common configuration mode

Usage Enabling DNS cache optimizes CPU utilization on the active ACOS device because most DNS requests get served directly through the cache. However, a failover event can cause the CPUs to spike on the standby ACOS device because the device has to resolve all destination hosts in bulk. This CPU spike becomes amplified if recursive DNS service is also enabled. Upon failover, the standby device stays ready to resolve DNS queries from cache.

Example The following example enables DNS synchronization:

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-sync
```

dns-cache-sync-entry-size

Description Configures DNS cache entries with smaller size to be synchronized to the standby device.

Syntax

```
[no] dns-cache-sync-entry-size
```

Default 256 bytes

Mode SLB common configuration mode

Usage This command can be configured only when global DNS cache synchronization is enabled.

The configurable range is 1-4096 bytes.

Example The following example enables synchronization of DNS cache entries that have size less than 500 bytes:

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-sync-entry-size 500
```

dns-cache-sync-ttl-threshold

Description Configures DNS cache entries with higher TTL value to be synchronized to the standby device.

Syntax

```
[no] dns-cache-sync-ttl-threshold
```

Default 0 seconds

Mode SLB common configuration mode

Usage This command can be configured only when global DNS cache synchronization is enabled.

The configurable range is 0-10000000 seconds.

Example The following example enables synchronization of DNS cache entries that have TTL value higher than 300 seconds:

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-sync-ttl-threshold 300
```

dns-cache-ttl-adjustment-enable

Description This option can be enabled for global DNS cache entries. When this option is enabled, the TTL value is updated to current TTL value when ACOS responds to a DNS query with the cached DNS response.

Syntax

```
[no] dns-cache-ttl-adjustment-enable
```

Default Disabled

Mode SLB common configuration mode

Example An example is mentioned below to enable the option for global DNS cache entries:

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-ttl-adjustment-enable
```

dns-cache-hitcount-enable

Description Globally enable hit count to global DNS cache entries.

Syntax

```
[no] dns-cache-hitcount-enable
```

Default The hit count to global DNS cache entries is disabled by default.

Mode SLB common configuration mode

Usage When the hit count to the global DNS cache is enabled, the ACOS device records the total number of hits made to the cache. The number of hits to each cache entry can be displayed in the `show dns cache entry` command.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-hitcount-enable
```

dns-cookie-cache-policy

Description Configures the global caching policy for filtering DNS requests and responses with cookie records.

Syntax

```
[no] dns-cookie-cache-policy {served-by-cache | served-by-backend}
```

Parameter	Description
served-by-cache	DNS queries with cookies are served from the DNS cache without the cookie record if a cache hit occurs.
served-by-backend	DNS queries with cookies are forwarded to the DNS backend server and the backend server responds to the queries with the cookie record regardless of cache status.

Default The `served-by-cache` option is enabled by default.

Mode SLB common configuration mode

Usage This command determines how DNS queries containing cookie records are handled, either by serving them from the cache (without the cookie record) or by forwarding them to the backend server (with cookie record). Configuring this policy at the global level allows ACOS clients to choose between optimizing performance using the cache or getting complete responses with cookie records by forwarding queries to the DNS backend server.

Example The following sample enables the policy for handling DNS queries with cookie records by serving them from the cache.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cookie-cache-policy served-by-cache
```

dns-max-udp-size

Description Configures the maximum DNS response size that ACOS is allowed to send over UDP globally.

Syntax

```
dns-max-udp-size <512-4096>
```

Default Not enabled

Mode SLB Common Configuration

Usage This command sets a global upper limit on the DNS UDP response size for all **dns-udp** type virtual-ports.

If a DNS response exceeds the configured size, ACOS sets the TC (truncated) bit in a minimal response and instructs the client to retry over TCP.

NOTE: The **dns-max-udp-size** value must be smaller than any **edns-udp-size** values defined without template-level **max-udp-size** in the same partition.

Example This example configures the global maximum UDP payload size:

```
ACOS(config)# slb common
ACOS(config-common)# dns-max-udp-size 1024
```

Related Commands:

- max-udp-size
- recursive-dns-resolution

dns-negative-cache-enable

Description Configures the caching of negative DNS responses at global level.

Syntax

```
[no] dns-negative-cache-enable [cache-non-valid]
```

Default Only valid negative responses are cached by default.

Mode SLB common configuration mode

Usage ACOS supports negative caching of the DNS response when it contains:

- CNAME records and SOA records
- NS records and SOA records
- Empty response and SOA records

By default, when **dns-negative-cache-enable** is configured, only valid negative responses are cached. These valid responses can be served directly from the cache if a matching query is received.

When the **cache-non-valid** option is configured, non-valid negative responses are also cached. However, while these non-valid responses are stored in the cache, they will not be served to DNS queries

Example The following example enables valid negative caching globally:

```
ACOS(config)# slb common
ACOS(config-common)# dns-negative-cache-enable
```

Example The following example enables both valid and non-valid negative caching globally:

```
ACOS(config)# slb common
ACOS(config-common)# dns-negative-cache-enable cache-non-valid
```

Related Commands:

- negative-dns-cache enable

dns-negative-cache-bypass-threshold

Description Specify the threshold for global negative cache responses to be served by the ACOS device.

Syntax

```
[no] dns-negative-cache-bypass-threshold num
```

Replace *num* with a threshold value between 1 - 65535.

Default The default value is 100.

Mode SLB common configuration mode

Usage For every threshold times the negative cache is served, the requests bypass the cache.

Example The following example configures the bypass threshold for negative caching globally:

```
ACOS(config)# slb common
ACOS(config-common)# dns-negative-cache-bypass-threshold 50
```

Related Commands:

- dns-negative-cache-enable

dns-persistent-cache-enable

Description Enables persistent storage for global DNS cache.

Syntax

```
[no] dns-persistent-cache-enable
```

Default Disabled

Mode SLB common configuration mode

Usage When the ACOS device restarts with empty cache, the CPU usage may spike, especially in the case of recursive DNS in production. When this option is enabled, the global DNS cache entries can be saved to a persistent storage which can be used to retrieve the previously cached entries when the ACOS device restarts.

Example The following example enables persistent DNS caching:

```
ACOS(config)# slb common
ACOS(config-common)# dns-persistent-cache-enable
```

dns-persistent-cache-hit-threshold

Description Sets the hit count threshold for persistent cache.

Syntax

```
[no] dns-persistent-cache-hit-threshold
```

Default Default value is 0.

Mode SLB common configuration mode

Usage Saves the DNS cache entries with higher hit count.

The value can be set from 0-10000000.

Example The following example displays the maximum persistent cache:

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
ACOS(config-common)#dns-persistent-cache-hit-threshold 5
```

dns-persistent-cache-ttl-threshold

Description Sets the TTL threshold value for persistent cache.

Syntax `[no] dns-persistent-cache-ttl-threshold`

Default Default value is 0.

Mode SLB common configuration mode

Usage Saves the DNS cache entries with higher TTL value.

The value can be set from 0-10000000.

Example The following example displays the maximum persistent cache:

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
ACOS(config-common)#dns-persistent-cache-ttl-threshold 200
```

dns-response-rate-limiting

Description Configures the DNS response rate limiting parameters for controlling resource usage.

Syntax `[no] dns-response-rate-limiting`

This command enters the DNS Response Rate Limiting configuration sub-mode where the following commands are available:

max-table-entries *num*	Specify the maximum number of entries allowed in the DNS rate-limiting table. It prevents the DNS attacks from consuming excessive system memory by limiting the

	number of entries the system can track for rate-limiting. If the number of entries exceeds the configured value, the older entries are automatically removed. It is a system-level command configured in Shared Partition.
source-entry-age *num*	Specify the duration for which a source entry remains active in the DNS rate-limiting table. The value is in minutes (1 - 60). Default value is 2 minutes. The source entries from the DNS rate-limiting table are removed once the configured value is exceeded, thereby releasing the allocated resources. This is a partition-level command.

Default Disabled by default.

Mode SLB common configuration mode

Example The following example sets the maximum number of table entries for DNS response rate limiting.

```
ACOS(config)# slb common
ACOS(config-common)# dns-response-rate-limiting
ACOS(config-common-dns-response-rate-limi...)# max-table-entries 2000
```

Example The following example sets the source-entry-age to 5 minutes.

```
ACOS(config)# slb common
ACOS(config-common)# dns-response-rate-limiting
ACOS(config-common-dns-response-rate-limi...)# source-entry-age 5
```

dns-vip-stateless

Description This command causes the ACOS device to use round-robin to load balance DNS stateless traffic to CPU threads.

NOTE: This command is only available on FTA-enabled platforms.

Syntax

```
[no] dns-vip-stateless
```

Mode SLB common configuration mode

Example Enable this feature:

```
ACOS(config)# slb common
ACOS(config-common)# dns-vip-stateless
```

drop-icmp-to-vip-when-vip-down

Description When a virtual IP is down it can still respond to ping (ICMP_ECHO) requests.

With this enabled, a virtual IP that is down will not respond to ping requests.

Syntax

```
[no] drop-icmp-to-vip-when-vip-down
```

Mode SLB common configuration mode

dsr-health-check-enable

Description Enable health checking of the virtual server IP addresses instead of the real server IP addresses in Direct server Return (DSR) configurations.

This feature requires configuration of a Layer 3 health method (ICMP), with the transparent option enabled, and the alias address set to the virtual IP address. (See method.) The health monitor must be applied to the real server ports.

Syntax

```
[no] dsr-health-check-enable
```

Default Health checking is disabled by default.

Mode SLB common configuration mode

Example The following commands configure a Layer 3 health monitor for DSR health checking, apply it to the real server ports, and enable DSR health checking:

```
ACOS(config)# health monitor dsr-hm
ACOS(config-health:monitor)# method icmp transparent
10.10.10.99
ACOS(config-health:monitor)# exit
ACOS(config)# slb common
ACOS(config-common)# dsr-health-check-enable
```

ecmp-hash

Description The option allows hashing on connection information (source IP, source port, destination port from forward tuple and real server IP), which would allow a more balanced (Equal-cost multi-path routing) protocol routing.

For IP based protocols, source IP and real server IP will be used for hashing. IPv4 to IPv6 or IPv6 to IPv4 routing is not supported.

Syntax

```
[no] ecmp-hash {system-default | connection-based}
```

Parameter	Description
system-default	Uses system default ecmp hashing algorithm.
connection-based	Uses connection information for hashing.

Mode SLB common configuration mode

Example The example mentioned below shows how to enable connection-based hashing:

```
ACOS(config)# slb common
ACOS(config-common)# ecmp-hash connection-based
```

NOTE: SSLi_L2 is not supported and smart nat is partially supported.

enable-l7-req-acct

Description Globally enable Layer 7 request accounting.

When using the least-request load-balancing method in a service group, Layer 7 request accounting is automatically enabled for the service group's members, and for the virtual service ports that are bound to the service group's members.

To display Layer 7 request statistics, use the **show slb service-group** command.

Syntax `[no] enable-l7-req-acct`

Default Disabled by default.

Mode SLB common configuration mode

Example The example below shows how to enable Layer 7 request accounting.

```
ACOS(config)# slb common
ACOS(config-common)# enable-l7-req-acct
```

Related Commands:

- show slb server
- show slb service-group
- show slb virtual-server

extended-stats

Description Globally enable collection of extended SLB statistics, including peak connection statistics.

Syntax `[no] extended-stats`

Default Disabled by default.

Mode SLB common configuration mode

Example This example shows how to enable the collection of extended SLB statistics.

```
ACOS(config)# slb common
ACOS(config-common)# extended-stats
```

fast-path-disable

Description Disable fast-path packet inspection.

Fast processing of packets maximizes performance by using all underlying hardware assist facilities. Typically, the feature should remain enabled. The disable option is provided only for troubleshooting, in case it is suspected that the fast processing logic is causing an issue. If you disable fast-path processing, ACOS does not perform a deep inspection of every field within a packet.

Syntax

```
[no] fast-path-disable
```

Default Enabled by default.

Mode SLB common configuration mode.

Example The example below shows how to disable fast-path packet inspection.

```
ACOS(config)# slb common
ACOS(config-common)# fast-path-disable
```

gateway-health-check

Description Enables gateway health monitoring.

Syntax

```
[no] gateway-health-check [interval seconds [timeout seconds]]
```

Parameter	Description
interval *second*	Specifies time period between health check attempts, 1-180 seconds. The default interval is 5 seconds.
timeout *seconds*	Specifies how long the ACOS device waits for a reply to any of the ARP requests, 1-360 seconds. The default timeout is 15 seconds.

Default See descriptions.

Mode SLB common configuration mode.

Usage Gateway health monitoring uses ARP to test the availability of nexthop gateways. When the ACOS device needs to send a packet through a gateway, the ACOS device begins sending ARP requests to the gateway.

- If the gateway replies to any ARP request within a configurable timeout, the ACOS device forwards the packet to the gateway.
- The ARP requests are sent at a configurable interval. The ACOS device waits for a configurable timeout for a reply to any request. If the gateway does not respond to any request before the timeout expires, the ACOS device selects another gateway and begins the health monitoring process again.

Example The following example enables gateway health monitoring. Health check attempts will be made every 10 seconds, with a reply timeout of 20 seconds.

```
ACOS(config)# slb common
ACOS(config-common)# gateway-health-check interval 10 timeout
20
```

global-dns-cache

Description Configures global DNS cache related settings.

Syntax `[no] global-dns-cache`

This command changes the CLI to the configuration level for the global DNS cache, where the following commands are available:

Parameter	Description
[no] class-list *class-list-name* **lid** *num* {**conn-rate-limit** *num* **per** *num* | **dns** *options* |	Specifies the classification list for the global DNS cache. The following sub-command is available: **lid** *num* - Configures a limit identifier within the class list. The value of *num* can range from 1-1023. This command changes the CLI to the configuration level for the LID, where the following sub-commands are available:

Parameter	Description
over-limit-action *options* | **user-tag**}	• **conn-rate-limit** *num* - Configures the maximum number of connection rate allowed. The number of connections *num* can range from 1-2147483647. ◦ **per** *num* – Configures the connection rate limit per 100ms. The interval *num* can range from 1-65535 seconds. • **dns** - Configures DNS cache options. The following *options* are available: ◦ **cache-disable** - Disables DNS cache. If the DNS cache is enabled at the SLB common (global) configuration level, this LID configuration takes precedence. ◦ **cache-enable** - Enables DNS cache. ◦ **honor-server-response-ttl** - Enables TTL in the server response to be used as DNS cache TTL. ◦ **ttl** - Configures TTL for cache entry. ◦ **weight** - Configures weight for cache entry. • **over-limit-action** - Configures the action when the connection rate limit is exceeded. The following *options* are available: ◦ **ignore** - Ignores the connection rate limit and proceeds. ◦ **log** *num* - Enables system logs to generate log messages for the ignored DNS query at the specified interval. The log interval *num* can range from 1-255 minutes. When logging is enabled: ◦ If *num* is not specified, a log message is generated for each over-limit occurrence.

Parameter	Description
	◦ If *num* is specified, a log message is generated for every *num* minutes irrespective of multiple over-limit occurrences. ◦ **drop** - Drops the DNS query when the connection rate limit exceeds. ◦ **lockout** *num* - Locks out the client for a specified number of minutes. During the lockout period, all connection requests from the client are dropped. The lockout period *num* can be 1-1023 minutes. There is no default value. ◦ **log** *num* - Enables system logs to generate log message for the dropped DNS query at the specified interval. The log interval *num* can range from 1-255 minutes. When logging is enabled: ◦ If *num* is not specified, a log message is generated for each over-limit occurrence. ◦ If *num* is specified, a log message is generated for every *num* minutes irrespective of multiple over-limit occurrences. • **user-tag** - Configures a customized tag.

Mode SLB common configuration mode

Usage When global DNS caching is enabled, the ACOS device can selectively bypass DNS cache entries according to specified domain names and/or source IPv4/IPv6 addresses. Additionally, limits can be imposed on the DNS queries per class-list based on limit identifiers. The Time-To-Live (TTL) duration can be configured for cache entries in order to manage the cached DNS data.

Global DNS caching is applied to DNS requests sent to both UDP and TCP virtual ports in a DNS SLB configuration.

Example The following example shows a global DNS cache configuration:

```
ACOS(config)# slb common
ACOS(config-common)# global-dns-cache
ACOS(config-common-global-dns-cache)# class-list cl_dns_cache
ACOS(config-common-global-dns-cache-class…)# lid 1
ACOS(config-common-global-dns-cache-class…)# dns cache-disable
ACOS(config-common-global-dns-cache-class…)# user-tag dns_
cache_bypass
ACOS(config-common-global-dns-cache-class…)# exit
ACOS(config-common-global-dns-cache-class…)# lid 2
ACOS(config-common-global-dns-cache-class…)# dns cache-enable
ACOS(config-common-global-dns-cache-class…)# dns ttl 1000
ACOS(config-common-global-dns-cache-class…)# user-tag entry_
manual_ttl
ACOS(config-common-global-dns-cache-class…)# exit
ACOS(config-common-global-dns-cache-class…)# exit
ACOS(config-common-global-dns-cache)# exit
ACOS(config-common)# exit
```

graceful-shutdown

Description Provides time for active sessions to terminate normally before closing a service after deleting or disabling the real or virtual server or port providing the service.

Syntax

```
[no] graceful-shutdown grace-period
[server | virtual-server] [after-disable]
```

Parameter	Description
grace-period	Number of seconds existing connections on a disabled or deleted server or port are allowed to remain up before being terminated. You can specify 1-65535 seconds.
server	Limits the graceful shutdown to real servers only.

Parameter	Description
virtual-server	Limits the graceful shutdown to virtual servers only.
after-disable	Applies graceful shutdown to disabled servers and service ports, as well as deleted servers. Without this option, graceful shutdown applies only to deleted servers.

Default Graceful shutdown is disabled by default. When you delete a real or virtual service port, the ACOS device places all the port's sessions in the delete queue, and stops accepting new sessions on the port.

Mode SLB common configuration mode.

Usage When graceful shutdown is enabled, the ACOS device stops accepting new sessions on a disabled or deleted port, but waits for the specified grace period before moving active sessions to the delete queue.

Example These commands enable graceful shutdown with a grace period of one hour:

```
ACOS(config)# slb common
ACOS(config-common)# graceful-shutdown 3600
```

honor-server-response-ttl

Description TTL in server response is used as DNS cache TTL.

Syntax

```
[no] honor-server-response-ttl
```

Mode SLB common configuration mode

Example The following example configures the ACOS device to cache DNS replies for 300 seconds.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-age 600
ACOS(config-common)# honor-server-response-ttl
```

hw-compression

Description Enable hardware-based HTTP compression.

Syntax `[no] hw-compression`

Default Disabled by default.

Mode SLB common configuration mode.

Usage Hardware-based compression is available using an optional hardware module on select platforms. For more information, see "Hardware-Based Compression" in the *Application Delivery Controller Guide*.

Example The following example enables hardware-based HTTP compression.

```
ACOS(config)# slb common
ACOS(config-common)# hw-compression
```

hw-syn-rr

Description Enable distribution of client SYNs across multiple CPUs. This feature protects against CPU overload due to SYN floods, a common symptom of DDoS attacks.

Syntax `[no] hw-syn-rr conn-num`

The *conn-num* option specifies the maximum number of connection requests (TCP SYNs) allowed from the same client (1-500000). If this threshold is exceeded, ACOS begins using all the CPUs for processing the SYNs.

Default Disabled by default.

Mode SLB common configuration mode.

Usage Only the control CPU is used for SYN processing.

When the conn-num threshold is exceeded, ACOS begins distributing the SYNs to the CPUs in round-robin fashion. The control CPU and all data CPUs are used.

Example The following example enables distribution of client SYNs across multiple CPUs, using 250,000 TCP SYNs as the threshold.

```
ACOS(config)# slb common
ACOS(config-common)# hw-syn-rr 250000
```

lb-method-hash

Description Defines the global load balancing using hash-based algorithm.

Syntax

```
lb-method-hash src-ip-only {ipv4-offset | ipv6-subnet} num
```

To negate this command, use the following syntax:

Syntax

```
lb-method-hash src-ip-only {ipv4-offset | ipv6-subnet} 0
```

Parameter	Description
src-ip-only ipv4-offset *num*	Specify the hashing value based on the source IP address. The value specifies how far into the string to begin hash calculation. The IPv4 offset masks off octets of the source IP for the purpose of internal server selection. The offset value range is 0–3. The following list explains the value and the associated mask on the source IP. • **0**: 1.1.1.1 • **1**: 0.1.1.1 • **2**: 0.0.1.1 • **3**: 0.0.0.1
src-ip-only ipv6-subnet *num*	Specify the hashing value based on the IPv6 subnet length, in bytes. The value specifies how far into the string to begin hash calculation. The IPv6 subnet masks off octets of the source IP for the purpose of internal server selection. The subnet range is 0-15 (bytes). For example, if the IPv6 address is **ABCD:EF01:2345:6789:CDEF:0123:4567:89AB:**, based on the **ipv6-subnet** configuration, the value and associated masking on source IP will work as follows:

Parameter	Description
	• 1: AB00:: • 2: ABCD:: • 3: ABCD:EF00:: • 4: ABCD:EF01::, and so on • 13: ABCD:EF01:2345:6789:CDEF:0123:4500:: • 14: ABCD:EF01:2345:6789:CDEF:0123:4567:: • 15: ABCD:EF01:2345:6789:CDEF:0123:4567:8900

Note: The value 0 indicates that no masking is done, and the entire string is displayed. You must reset the value manually. The **no** prefix cannot be used to negate this command.

Mode SLB common configuration mode

Example In the following example IPv4 offset is set as 2 for the load balancing hash:

```
ACOS(config)# slb common
ACOS(config-common)# lb-method-hash src-ip-only ipv4-offset 2
```

Example In the following example, the IPv6 subnet is set as 10 for the load balancing hash:

```
ACOS(config)# slb common
ACOS(config-common)# lb-method-hash src-ip-only ipv6-subnet 10
```

Related Commands

- slb template udp

l2l3-trunk-lb-disable

Description Disable or re-enable trunk load balancing.

Syntax

```
[no] l2l3-trunk-lb-disable
```

Default Enabled by default.

Mode SLB common configuration mode.

Usage When trunk load balancing is enabled, the ACOS device load balances outbound Layer 2/3 traffic among all the ports in a trunk. The round-robin method is used to load balance the traffic. For example, in a trunk containing ports 1-4, the first Layer 2/3 packet is sent on port 1. The second packet is sent on port 2. The third packet is sent on port 3, and so on.

If you disable trunk load balancing, the lead port will always used for outbound traffic, and the other ports will act as standby ports in case the lead port goes down.

Trunk load balancing applies only to Layer 2/3 traffic, and is enabled by default. However, the CLI provides a command to disable trunk load balancing, in case there is a need to do so. Disabling trunk load balancing causes the ACOS device to use only the lead port for outbound traffic.

NOTE: Trunk load balancing does not apply to Layer 4-7 traffic.

Example The following commands disable trunk load balancing.

```
ACOS(config)# slb common
ACOS(config-common)# l2l3-trunk-lb-disable
```

max-buff-queued-per-conn

Description Set the maximum buffer threshold per connection.

Syntax

```
[no] max-buff-queued-per-conn buffer-value
```

Specify the desired *buffer-value* (128-4096).

Mode SLB common configuration mode.

Example The following commands set the maximum buffer value per connection to 1024:

```
ACOS(config)# slb common
ACOS(config-common)# max-buff-queued-per-conn 1024
```

max-http-header-count

Description Configure the number of headers supported in an HTTP request.

Syntax `[no] max-http-header-count num`

Replace *num* with the maximum number of HTTP headers supported within a request (90-255).

Default 90

Mode SLB common configuration mode

Example The following commands configure 90 as the number of headers supported in an HTTP request.

```
ACOS(config)# slb common
ACOS(config-common)# max-http-header-count 90
```

max-persistent-cache

Description Maximum persistent cache entries can be limited using this option.

Syntax `[no] max-persistent-cache`

Default Disabled

Mode SLB common configuration mode

Usage The option can be configured only in a shared partition. The maximum value is the maximum supported DNS cache on the platform.

Example The following example displays the maximum persistent cache on the platform used:

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
ACOS(config-common)#max-persistent-cache ?
<1-65536> Maximum persistent cache entry
```

msl-time

Description Configure the maximum session life for client sessions. The maximum session life controls how long the ACOS device maintains a session table entry for a client-server session after the session ends.

Syntax `[no] msl-time seconds`

The *seconds* option specifies the number of seconds a client session can remain in the session table after session completion. You can specify 1-39 seconds.

Default 2 seconds

Mode SLB common configuration mode

Usage The maximum session life allows time for retransmissions from clients or servers, which can occur if there is an error in a transmission. If a retransmission occurs while the ACOS device still has a session entry for the session, the ACOS device is able to forward the retransmission. However, if the session table entry has already aged out, the ACOS device drops the retransmission instead.

Maximum session life begins aging out a session table entry when the session ends:

- TCP – The session ends when the ACOS device receives a TCP FIN from the client or server.
- UDP – The session ends after the ACOS device receives a server response to the client's request. If the reply is fragmented, the maximum session life begins only after the last fragment is received.

NOTE: For UDP sessions, maximum session life is used only if UDP aging is set to short, instead of immediate. UDP aging is set in the UDP template bound to the UDP virtual port. The default setting is short.

Example The following commands configure a maximum session life of 10 seconds.

```
ACOS(config)# slb common
ACOS(config-common)# msl-time 10
```

mss-table

Description Configure the TCP Maximum Segment Size (MSS) allowed for client traffic. This command globally changes the MSS. You also can change the MSS in individual slb template tcp-proxy.

Syntax

```
[no] mss-table num
```

The *num* option specifies maximum MSS allowed in traffic from clients. You can specify 128-750.

Default 538

Mode SLB common configuration mode

Usage Clients who can only transmit TCP segments that are smaller than the MSS are unable to reach servers.

Example The following commands configure a TCP MSS of 256.

```
ACOS(config)# slb common
ACOS(config-common)# mss-table 256
```

ng-waf

Description Configure A10 Next-Gen WAF (NGWAF) settings.

Syntax

```
[no] ng-waf [ attack-resp-code resp_code | attack-resp-message { msg | custom-page page } | custom-signal-clist string_list | monitor-mode-enable | pre-process-enable exp_time | use-https-proxy { { ipv4_address | ipv6_address } portnum} | use-mgmt-port ]
```

Parameter	Description
attack-resp-code *resp_code*	Specify a custom response code i.e., an HTTP status code (400 to 599) to be returned when a request is blocked by NGWAF. **NOTE:** The custom response code on the Fastly Dashboard supersedes this setting i.e., this setting is ignored if you specify a response code on the Fastly Dashboard. By default, a response code 410 is returned if no response code is set on the Fastly dashboard or the Thunder device (using this option).
attack-resp-message *msg*	Display a custom message when a request is blocked by NGWAF. The message can be displayed

Parameter	Description
custom-page *page*	by specifying one of the following: • *msg* - A block message with a maximum length of 1023 characters. • **custom-page** *page* - An HTML webpage that contains the message to be displayed. **NOTE:** Ensure that you import the HTML webpage (using **import ng-waf-custom-page** command) to the shared partition or an L3V partition before executing this command. You can also add some relevant information to the message or webpage by using the reserved keywords that display the attack type, the time, the session ID, and the URI as well. The following keywords are available: • **$a10_ngwaf_attack_type$** - The reason for blocking the request or the attack type. For e.g., XSS, SQLI, or custom signals • **$a10_ngwaf_time$** - The time when the request is blocked. • **$a10_ngwaf_session_id$** - The session ID. • **$a10_ngwaf_uri$** - The request URI. **NOTE:** The keywords are case-sensitive and only 4 keywords can be used in a message or custom webpage.
custom-signal-clist *string_list*	Reserve and track certain custom signals by creating a class-list and binding it to NGWAF.

Parameter	Description
	NOTE: The class-list cannot have more than 64 entries.
monitor-mode-enable	Enable NGWAF monitor mode. When this mode is enabled, all the requests are monitored and allowed to pass; they are not blocked. However, the malicious requests, that would otherwise be blocked, are highlighted in the Syslogs and debug logs using the **marked** keyword. **NOTE:** The monitor mode overrides the Fastly rules configured to block and redirect requests, i.e., the Fastly rules are ignored when the monitor mode is enabled on the Thunder device.
pre-process-enable *exp_time*	Enable the NGWAF cache function to speed up the processing time. When this option is configured, the checked and forwarded requests are stored in the cache. Thereafter, similar requests are forwarded directly (without NGWAF checking). This option is disabled by default. **NOTE:** Blocked requests are not stored in the cache. *exp_time* - Specify the expiration time (1 to 480 minutes) for the cache entries. The default value is 1 minute. Additionally, all cache entries are freed if the partition is disabled or deleted.
use-https-proxy { *ipv4_address*	Connect to the Fastly Cloud through an explicit proxy server. By default, the connection to the Fastly Cloud is proxy-free.

Parameter	Description
| *ipv6_address* } *portnum*	Specify the following parameters: • *ipv4_address* - Proxy server IPv4 address OR *ipv6_address* - Proxy server IPv6 address • *portnum* - The port number (1-65534) **NOTE**: • Ensure that the specified explicit proxy server is reachable. • NGWAF (if enabled) will restart automatically after configuring or deleting the explicit proxy server.
use-mgmt-port	Connect to the Fastly Cloud through the management interface instead of the data interface (default route). **NOTE:** This command is only available on the shared partition but is applied to all partitions.

Default See descriptions.

Mode SLB common configuration mode.

Usage Although this command is under SLB Common, all the sub-commands can also be configured separately for each partition. Therefore, the shared partition and the L3V partitions can have different NGWAF settings.

Example The following example enables the NGWAF cache function and sets the cache expiration time to 5 minutes:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf pre-process-enable 5
```

Example The following example sets the custom attack response code to 456:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-code 456
```

Example The following example enables the NGWAF monitor mode:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf monitor-mode-enable
```

Example The following example sets a custom message to be displayed when a request is denied:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message "The request
is denied!\n"
```

Example The following example sets a custom message using the reserved keyword:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message "The request
is blocked!\n Additional Information\n URI:$a10_ngwaf_uri$,
time:$a10_ngwaf_time$, attack:$a10_ngwaf_attack_type$, session
ID:$a10_ngwaf_session_id$\n"
```

Example output with keywords replaced:

```
The request is blocked!
Additional Information
URI:/pruducts?category=Gifts'--, time:2022-09-20-T06:49:43Z,
attack:SITE-FLAGGED-IP,SQLI, session
id:632962885477430a344ea0ee
```

Example The following example configures a custom webpage to be displayed when a request is denied:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message custom-page
mypage
```

Example The following example creates a class-list and binds it to NGWAF to track custom signals:

```
ACOS(config)# class-list signal_list string
ACOS(config-class list)# str site.login
```

```
ACOS(config-class list)# str site.error
ACOS(config-class list)# str site.logout

ACOS(config)# slb common
ACOS(config-common)# ng-waf custom-signal-clist signal_list
```

Example The following example enables connection through the specified IPv4 proxy server:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-https-proxy 192.168.2.2 3128
```

Example The following example enables connection through the specified IPv6 proxy server:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-https-proxy 2022:192::33 3128
```

Example The following example enables management interface usage for NGWAF:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-mgmt-port
```

no-auto-up-on-aflex

Description Prevent the health status of virtual ports that are bound to aFleX scripts from being automatically marked Up.

Syntax

```
[no] no-auto-up-on-aflex
```

Default This option is disabled by default. Virtual ports that are bound to aFleX scripts are automatically marked Up.

Mode SLB common configuration mode

Example The following commands prevent the health status of virtual ports that are bound to aFleX scripts from being automatically marked Up.

```
ACOS(config)# slb common
ACOS(config-common)# no-auto-up-on-aflex
```

odd-even-nat-enable

Description On a Multi-PU platform, such as TH7650 or TH7655S, this command utilizes the client-side and server-side (odd-even NAT) IP addresses to determine the traffic distribution to PU1 and PU2. This means that traffic sent from an odd source IP to the same VIP is sent to PU1, while traffic sent from an even source IP to the same VIP is sent to PU2. This allows a single SLB virtual server to be shared across both PUs.

Prerequisite To implement Multi-PUs, you must configure the traffic-distribution-mode option in the vlan or interface command.

Limitation Forward and Reverse traffic needs to be symmetric per PU. For example, the traffic-distribution-mode options on the client or server interface pair can be sip/dip, primary/primary, and blade/blade.

NOTE: It is recommended to configure sip/dip for better performance on dual Multi-PU platforms because traffic will be distributed to both PUs.

Syntax

```
[no] odd-even-nat-enable
```

Default Not configured

Mode SLB Common

Usage This command is used by Multi-PU platforms such as TH7650 or TH7655S to allow for a more even traffic distribution over all available PUs (Processing Units). This command should be used in conjunction with the **traffic-distribution-mode** command to process forward and reverse traffic from the same session by the same PU.

This means that the traffic sent from an odd source IP to the same VIP, is sent to the PU1, whereas traffic sent from an even source IP to the same VIP, is sent to the PU2. The SLB virtual servers can thus operate in the active-active mode.

For complete ADC Multi-PU configuration, see *Application Delivery Controller Guide*.

Example The following command enables this command:

```
ACOS(config)# slb common
ACOS(config-common)# odd-even-nat-enable
```

Related Commands:

- vlan
- interface

pbslb-entry-age

Description Modify the global PBSLB entry age in minutes.

Syntax

```
[no] pbslb-entry-age minutes <1-127>
```

Default 6 minutes

Usage The PBSLB entries are expired or removed after aging out.

- If the PBSLB entries current age is less than the set value, then it is updated to the new value on the next traffic.
- If the PBSLB entries current age is greater than the set value, then it will remain in that value.

This setting is beneficial when the CPU consumption is high due to large number of PBSLB entries. Hence, lower the PBSLB entry age better is the CPU performance.

Mode SLB Common Configuration

Example The following command configures the PBSLB entry age:

```
ACOS(config)# slb common
ACOS(config-common)# pbslb-entry-age 2
ACOS(config-common)# exit
```

Related Commands:

- show pbslb

rate-limit-logging

Description Configure rate limiting settings for system logging.

Syntax

```
[no] rate-limit-logging
[max-local-rate msgs-per-second]
[max-remote-rate msgs-per-second]
[exclude-destination {local | remote}]
```

Parameter	Description
max-local-rate *msgs-per-second*	Specifies the maximum number of messages per second that can be sent to the local log buffer. You can specify 1-500. The default is 64 messages per second.
max-remote-rate *msgs-per-second*	Specifies the maximum number of messages per second that can be sent to remote log servers. You can specify 1-1,000,000. The default is 15000 messages per second.
exclude-destination	Excludes logging to the specified destination, local or remote. By default, logging to both destinations is enabled.

Default See descriptions.

Mode SLB common configuration mode.

Usage Log rate limiting is enabled by default and can not be disabled. The configurable settings have the default values as described in the table above.

The log rate limiting mechanism works as follows:

- If the number of new messages within a one-second interval exceeds the internal maximum (64 by default), then during the next one-second interval, ACOS sends log messages only to the external log servers.
- If the number of new messages generated within the new one-second interval is the internal maximum or less, then during the following one-second interval, ACOS will again send messages to the local logging buffer as well as the external log server.
- In any case, all messages (up to the external maximum) are sent to the external log servers.

Example The following commands increase the maximum number of log messages per second sent to remote log servers:

```
ACOS(config)# slb common
ACOS(config-common)# rate-limit-logging max-remote-rate 30000
```

recursive-ns-cache

Description Configures TTL settings for NS cache entry.

Syntax

```
[no] recursive-ns-cache  <option>
```

The following options are available:

Parameter	Description
honor-packet-ttl	This is the default option. Configuring this option sets the TTL for NS records cache entry based on the lowest TTL among all the NS records from the server's response.
honor-age-con-fig	Configuring this option sets the TTL value based on the DNS cache configuration that is set on the device using commands such as `dns-cache-age`, `honor-server-response-ttl`.

Default `honor-packet-ttl`

Mode SLB common configuration mode

Usage DNS cache should be enabled using the dns-cache-enable command. Both the parameters are mutually exclusive, and only one can be configured.

Example This example configures option `honor-age-config`.

```
ACOS(config)# slb common
ACOS(config-common)# dns-cache-enable
ACOS(config-common)# dns-cache-entry-size 4096
ACOS(config-common)# recursive-ns-cache honor-age-config
```

reset-stale-session

Description Send reset if a session in the delete queue receives a SYN packet.

Syntax

```
[no] reset-stale-session
```

Mode SLB common configuration mode.

Example The following command enables this feature.

```
ACOS(config)# slb common
ACOS(config-common)# reset-stale-session
```

scale-out

Description Enable the Scaleout feature for SLB.

For more information, see the *Configuring Scaleout* guide.

Syntax

```
[no] scale-out
```

Default Not enabled.

Mode SLB common configuration mode.

service-group-on-no-dest-nat-vports

Description Bind one service-group under multiple virtual-server when 'no-dest-nat' is enabled.

Limitation Health check operating in DSR mode is incompatible if a user enables **dsr-health-check-enable** and binds same service-group on multiple **no-dest-nat** virtual ports.

Syntax

```
[no] service-group-on-no-dest-nat-vports [allow-same |
enforce-different]
```

Parameter	Description
allow-same	Allow the binding service-group on no-dest-nat virtual ports.
enforce-different	Enforce that the same service-group can not be bound on different **no-dest-nat** virtual ports. This configuration is supported in both shared and L3V partitions

Mode SLB Common

Usage In some cases, there may be a specific requirement where user must bind one service-group under multiple virtual-server with 'no-dest-nat' enabled.

Example The following example configures this command:

```
ACOS(config)# slb common
ACOS(config-common)# service-group-on-no-dest-nat-vports
allow-same
```

snat-gwy-for-l3

Description Enable this option to use the default gateway of an IP source NAT pool to forward the traffic from a real server.

Syntax

```
[no] snat-gwy-for-l3 allow-in-gateway-mode
```

Parameter	Description
snat-gwy-for-l3	This option should be used in transparent mode to forward layer 3 traffic using the default gateway of an IP source NAT pool.
allow-in-gateway-mode	This option should be used in gateway mode to forward layer 3 traffic using the default gateway of an IP source NAT pool.

Default Disabled.

Mode SLB common configuration mode.

Usage When this option is enabled, the ACOS device checks the configured IP NAT pools from a range of IP addresses that includes the server IP address. If the pool's address range includes the server's IP address (same subnet), and the pool's default gateway is defined, the ACOS device routes server traffic through the pool's default gateway.

Example The following commands enable traffic forwarding in the transparent mode.

```
ACOS(config)# slb common
ACOS(config-common)# snat-gwy-for-l3
```

Example The following commands enable traffic forwarding in the gateway mode.

```
ACOS(config)# slb common
ACOS(config-common)# snat-gwy-for-l3 allow-in-gateway-mode
```

Related Commands:

- ip nat pool

snat-on-vip

Description Globally enable IP NAT support for VIPs.

Syntax

```
[no] snat-on-vip
```

Default Disabled by default.

Mode SLB common configuration mode

Usage Source IP NAT can be configured on a virtual port in the following ways:

- ACL-based source NAT (access-list command at virtual port level)
- VIP source NAT (slb snat-on-vip command at Configuration mode level)
- aFleX policy (aflex command at virtual port level)
- Non-ACL source NAT (source-nat command at virtual port level)

These methods are used in the order shown above. For example, if IP source NAT is configured using an ACL on the virtual port, and the slb snat-on-vip command is also used, then a pool assigned by the ACL is used for traffic permitted by the ACL. For traffic not permitted by the ACL, VIP source NAT can be used instead.

The current release does not support source IP NAT on FTP or RTSP virtual ports.

Example The following commands enable IP NAT support for VIPs.

```
ACOS(config)# slb common
ACOS(config-common)# snat-on-vip
```

sort-res

Description Enable the sort display option for SLB configuration. When this option is enabled, SLB resources in the configuration are listed in alphabetical order.

The sort feature takes effect only after you configure at least one SLB resource, after you enable the sort feature. Before you configure at

least one new SLB resource, the SLB resources still appear in the order they were configured.

Syntax

```
[no] sort-res
```

Default This option is disabled by default. With this default behavior, SLB resources of a specific type appear in the order they are configured.

Mode SLB common configuration mode

Example The following command displays the configured SLB servers, before the sort option is enabled and activated:

```
ACOS(config-common)#  show running-config | include slb server
slb server ee 5.5.5.5
slb server rs20_10 20.20.20.10
slb server Server07 110.20.20.20
slb server Server08 110.13.13.20
slb server MSSQLServer02 110.13.13.21
slb server srv266 10.10.100.10
slb server srv238 2.1.1.238
slb server rs_http 10.1.2.10
slb server ldap-sr 172.16.2.10
slb server s1 20.20.20.30
slb server woo 10.10.99.99
slb server o1 10.10.10.5
slb server http1 20.20.25.10
slb server http2 20.20.25.11
```

These commands enable the sort option, configure a new SLB server, and display the configured SLB servers. The slb server commands are alphabetically sorted.

```
ACOS(config)# slb common
ACOS(config-common)# sort-res
ACOS(config-common)#  exit
ACOS(config)#  slb server s88 4.3.3.3
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# show run | include slb
server
slb server MSSQLServer02 110.13.13.21
slb server Server07 110.20.20.20
slb server Server08 110.13.13.20
```

```
slb server ee 5.5.5.5
slb server fsort2 4.3.9.58
slb server fsort88 4.3.9.55
slb server http1 20.20.25.10
slb server http2 20.20.25.11
slb server ldap-sr 172.16.2.10
slb server o1 10.10.10.5
slb server rs20_10 20.20.20.10
slb server rs_http 10.1.2.10
slb server s1 20.20.20.30
slb server s88 4.3.3.3
slb server srv238 2.1.1.238
slb server srv266 10.10.100.10
slb server woo 10.10.99.99
slb server zsort2 4.3.3.9
ACOS(config-real server-node port)#
```

ssl-module

Description Switch the SSL module modes.

Syntax

```
[no] ssl-module
```

Parameter	Description
N5-new	Switch to Hardware-assisted Nitrox V (N5) SSL module with TLS 1.2 and 1.3 support using OpenSSL 1.1.1.
QAT	Switch to Hardware-assisted QuickAssist Technology (QAT) SSL module.
QAT4	Switch to Hardware-assisted QuickAssist Technology (QAT) generation 4 SSL module. This command is specifically designed for Dell MVP R760 SSL Offload capabilities.
software	Switch to Software-assisted SSL module.
software-tls13	Switch to Software-assisted SSL module with TLS 1.3 support.

Parameter	Description
`software-tls13-off-load`	Switch to Software-assisted SSL module with CPU offload support. Refer to the 'Usage' section below to understand the SSL offload process. **NOTE:** • Make sure to configure the offload-cpus command. • If the software-tls13 and QAT is already configured, then it is not required to reboot the system for the changes to take effect.

Default SSL module is not configured.

Mode SLB common configuration mode

Usage The following process describes the SSL offload engine workflow:

1. SSL Offload Engine will allocate and initialize a buffer with all the relevant data for the SSL Crypto operation.
2. On the CPU Offload, the SSL Crypto operation is executed.
3. On the home Data CPU, the SSL packet processing is resumed.

NOTE:

- QAT and N5 options are SSL hardware-assisted acceleration modules and not on-board SSL processors.
- Reboot the system after configuring the option to take effect.
- If supported elliptic curve extensions are not provided during ECC cipher negotiation, connection failures may occur with **ssl-module QAT** or **ssl-module software-tls13**. In such cases, using **ssl-module software** is recommended to ensure successful negotiation, in line with OpenSSL 1.1.1 behavior.
- It is recommended to avoid using the **[no] ssl-module** command unless it is absolutely necessary. Always test such configuration changes in a test environment before implementing them in the production environment.

Example The following command enables the SSL module QAT:

```
ACOS(config)#slb common
ACOS(config-common)#ssl-module QAT
```

ssli-sni-hash-enable

Description Relays SNI information without interfering the message (A10-FP header). Supports dynamic-port, single-device, and two-partition SSLi.

Syntax **[no] ssl-sni-hash-enable**

Default Disabled

Mode SLB common configuration mode

Usage Dynamic-port SSLi requires proprietary messaging to relay the SNI information from the inside SSLi virtual service to the outside SSLi virtual service. This messaging may interfere with the inspection devices that intercept and inspect decrypted traffic.

To enable this feature for two-device dynamic port deployment or the security device that modifies the IP address or port number, use the ssli-sni-hash-enable clientside-ip | clientside-ipv6 and ssli-sni-hash-

enable serverside-ip | serverside-ipv6 options to relay the SNI information.

Example The following commands relay the SNI information without interfering the message (A10-FP header).

```
ACOS(config)# slb common
ACOS(config-common)# ssli-sni-hash-enable
```

Related Commands:

- ssli-sni-hash-enable clientside-ip | clientside-ipv6
- ssli-sni-hash-enable serverside-ip | serverside-ipv6

ssli-sni-hash-enable clientside-ip | clientside-ipv6

Description Configure the client-side (ACOS_decrypt) management IP and port number on the server-side (ACOS_encrypt) to relay the SNI information.

Prerequisite

- Enable the ssli-inbound-enable command on the client SSL template.
- Configure the ssli-sni-hash-enable serverside-ip | serverside-ipv6 command on the client-side.

Syntax

```
[no] ssli-sni-hash-enable {clientside-ip ipv4-address |
clientside-ipv6 ipv6-address} port port-number
```

Parameter	Description
clientside-ip *ipv4-address*	Specify the IPv4 address of the client-side.
clientside-ipv6 *ipv6-address*	Specify the IPv6 address of the client-side.
port *port-number*	Specify the protocol port number of the server-side for SNI information transmission. The value can be from 1-65535.

Parameter	Description
	Avoid using common port numbers like 22, 80, and 443.

Default Not enabled

Mode SLB common configuration

Usage Configure this command, if you have a two-device deployment and want to relay the SNI information from the client-side inbound SSLi to the server-side outbound SSLi. Configure the management IP address of both the devices to set up a TCP connection to relay the SNI information.

- If the connection is not established between the client-side and server-side for SNI transmission, the server-side application connection will be terminated.
- If the server-side does not receive the SNI information in time, the server-side application connection will be terminated.

Example The following example configures the client-side information to relay the SNI information to the server-side:

```
ACOS(config)# slb common
ACOS (config-common)# ssli-sni-hash-enable clientside-ip
10.65.18.200 port 5555
```

NOTE: It is recommended to configure either the IPv4 or IPv6 management IP addresses on both the devices.

Related Commands:

- ssli-inbound-enable
- ssli-sni-hash-enable serverside-ip | serverside-ipv6

ssli-sni-hash-enable serverside-ip | serverside-ipv6

Description Configure the server-side (ACOS_encrypt) management IP address and port number on the client-side (ACOS_decrypt) to relay the SNI information.

Prerequisite

- Enable the ssli-inbound-enable command on the client SSL template.
- Configure the ssli-sni-hash-enable clientside-ip | clientside-ipv6 command on the client-side.

Syntax

```
[no] ssli-sni-hash-enable {serverside-ip ipv4-address |
serverside-ipv6 ipv6-address} port port-number
```

Parameter	Description
serverside-ip *ipv4-address*	Specify the IPv4 address of the server-side.
serverside-ipv6 *ipv6-address*	Specify the IPv6 address of the server-side.
port *port-number*	Specify the protocol port number of the server-side for SNI information transmission. The value can be from 1-65535. Avoid using common port numbers like 22, 80, and 443.

Default Not enabled

Mode SLB common configuration

Usage Configure this command, if you have a two-device deployment and want to relay the SNI information from the client-side inbound SSLi to the server-side outbound SSLi. Configure the management IP address of both the devices to set up a TCP connection to relay the SNI information.

- If the connection is not established between the client-side and the server-side for SNI transmission, the server-side application connection will be terminated.
- If the server-side does not receive the SNI information in time, the server-side application connection will be terminated.

Example The following example configures the server-side information to relay the SNI information to the client-side:

```
ACOS(config)# slb common
ACOS (config-common)# ssli-sni-hash-enable serverside-ip
10.65.18.199 port 5555
```

NOTE: It is recommended to configure either the IPv4 or IPv6 management IP addresses on both the devices.

Related Commands:

- ssli-inbound-enable
- ssli-sni-hash-enable clientside-ip | clientside-ipv6

ssli-silent-termination-enable

Description Enable terminating SSLi sessions without sending the RST or FIN packets to the client or server.

This command is configured per partition.

Prerequisite

- Enable enable-l7-req-acct command to enable Layer 7 request accounting.

Syntax

```
[no] ssli-silent-termination-enable
```

Default Disabled

Mode SLB common configuration mode

Usage If this command is enabled and a client-SSL or server-SSL template is bound to the virtual port, the RST or FIN packets will not be sent when the **idle-timeout**, **close-notify**, or **clear session** commands are triggered.

NOTE: Enabling this feature may cause sessions to stall on either the client or the server side.

Example Enable the command:

```
ACOS(config)#  slb common
ACOS(config-common)# enable-l7-req-acct
ACOS(config-common)# ssli-silent-termination-enable
```

stateless-sg-multi-binding

Description Globally enables the device to allow the binding of stateless service groups by multiple virtual ports or virtual servers.

After a stateless service group is bound to multiple entities, this command can be deleted only after all multiple binding instances are removed.

Syntax

```
[no] stateless-sg-multi-binding
```

Default Disabled

Mode SLB common configuration mode

Example The following commands enable the binding of stateless service groups to multiple virtual ports or servers.

```
ACOS(config)# slb common
ACOS(config-common)# stateless-sg-multi-binding
```

stats-data-disable

Description Globally disables periodic collection of statistical data for system resources, including CPU, memory, disks and interfaces.

Syntax

```
[no] stats-data-disable
```

Default Disabled (statistics collection is enabled)

Mode This command is applicable to the following configuration modes

- SLB common
- SLB port template
- SLB server template
- Real server
- Service group
- Virtual server
- Virtual port

Example The following commands globally disable statistics collection for system resources.

```
ACOS(config)# slb common
ACOS(config-common)# stats-data-disable
```

use-mss-tab

Description Configure ACOS to base the MSS in replies from VIPs to clients on the interface MTU and MSS value received from clients in SYNs.

Syntax

```
[no] use-mss-tab
```

Default Disabled by default.

Mode SLB common configuration mode

slb forward-proxy

Description Configure the forward proxy objects as additional actions that will be bound to the forward-policy advance match rules.

Syntax

```
[no] slb forward-proxy {notify-page name | time-range}
```

Command	Description
notify-page *name* {*message*}	Sends a notification or response web page to the client. This command changes the CLI to 'notify-page' sub-configuration mode, where you can configure a response `message`. The string message can be between 1-1023 characters. HTML tags are included, and quotation marks are required for white spaces. When an HTTP request hits a match rule with this additional action, ACOS will notify the client before forwarding the request as the primary action of the rule. Each partition can have a maximum of 50 notify-page instances. However, each layer 4 connection only gets

Command	Description
	the notification once. • This action will become inactive during SNI or SAN filtering. • This action notifies only for HTTP GET, POST, PUT, and DELETE methods.
time-range *{options}*	Specify the time-range condition during which the client's request can be accepted or dropped. This command changes the CLI to 'time-range' sub-configuration mode, where the commands in Table 21 are available. Each partition can have a maximum of 50 time-range instances.

Table 21 : Sub-Commands in the time-range Configuration Mode

Command	Description
`daily [hh:mm to hh:mm]`	Specify the daily time range when the advance match condition will be applied. The time is *hh:mm* 24-hours local time format.
`days-of-month [num to num]`	Specify the day in a month when the advance match condition will be applied. The day is *num* to *num* format, which can be between 1-31.
`months-of-year [num to num]`	Specify the month in a year when the advance match condition will be applied. The month is *num* to *num* format, which can be between 1-12.
`use-utc-time`	Enable the Coordinated Universal Time (UTC) standard when the advance match condition will be applied.

Table 21 : Sub-Commands in the time-range Configuration Mode

Command	Description
weekday-fr	Apply the match conditions every Friday.
weekday-mo	Apply the match conditions every Monday.
weekday-sa	Apply the match conditions every Saturday.
weekday-su	Apply the match conditions every Sunday.
weekday-th	Apply the match conditions every Thursday.
weekday-tu	Apply the match conditions every Tuesday.
weekday-we	Apply the match conditions every Wednesday.

Default NA

Mode Global Configuration

Usage Set up a response web page and message to notify the client that the access will be monitored. Similarly, set up a time range when the requests will be forwarded or dropped. After setting up the options, you must bind the match-type condition to the **destination adv-match** rule in the **forward-policy** template.

Example The following example configures the time range for every Monday to Friday from January to April.

```
ACOS(config)# slb forward-proxy time-range Office_Hours
ACOS(config-time-range:OfficeHours)# weekday-mo
ACOS(config-time-range:OfficeHours)# weekday-tu
ACOS(config-time-range:OfficeHours)# weekday-we
ACOS(config-time-range:OfficeHours)# weekday-th
ACOS(config-time-range:OfficeHours)# weekday-fr
ACOS(config-time-range:OfficeHours)# months-of-year 1 to 4
```

Example The following example configures the notify page and response message.

```
ACOS(config)# slb forward-proxy notify-page Test
ACOS(config-notify-page:Test)# message "Request to a
restricted URL"
```

Example The following example binds the forward-proxy objects to the destination advance match rule.

```
ACOS(config)# slb template policy TEST
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# enable-adv-match
ACOS(config-policy-forward-policy)# source TEST_ICAP
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination adv-match 900
ACOS(config-policy-forward-policy-source-...)# match-time-range Office_Hours
ACOS(config-policy-forward-policy-source-...)# notify-page
```

Related Commands:

- slb template policy
- forward-policy

slb resource-usage

Description Change the capacity of an SLB resource.

Syntax

```
[no] slb resource-usage resource-type
```

Resource Type	Description and Acceptable Values
cache-template-count	Total number of configurable HTTP cache templates (32-2048) in the system.
client-ssl-template-count	Total number of configurable client SSL templates (32-8192) in the system.
conn-reuse-template-count	Total number of connection reuse templates (32-4096) in the system.
fast-tcp-	Total number of configuration Fast TCP templates (32-

Resource Type	Description and Acceptable Values
template-count	4096) in the system.
fast-udp-template-count	Total number of configuration Fast UDP templates (32-4096) in the system.
fix-template-count	Total number of configurable FIX templates (32-4096) in the system.
health-monitor-count	Total number of configurable health monitors (512-16384) in the system. **NOTE:** While configuring health monitors with the maximum configurable value, it is recommended to use multi-ctrl-cpu and set an appropriate value in the `multi-process` and `interval` parameters. For details, see health global.
http-template-count	Total number of configurable HTTP templates (32-4096).
link-cost-template-count	Total number of configurable Link-cost templates in the system.
log-template-count	Total number of configurable SLB Logging Templates in the System.
nat-pool-addr-count	Total number of source IP NAT pools (500-2000) in the system (deprecated).
pbslb-entry-count	Total number of configurable PBSLB entry in the system.
pbslb-	Total number of PBSLB subnets in the system

Resource Type	Description and Acceptable Values
subnet-count	(number depends on the amount of memory on your system).
persist-cookie-template-count	Total number of persistent cookie templates (32-4096) in the system.
persist-srcip-template-count	Total number of persistent source IP templates (32-4096) in the system.
proxy-template-count	Total number of configurable proxy templates (32-4096) in the system.
real-port-count	Total number of real server ports (512-16384) in the system. **NOTE:** GSLB resource limit considers the limit set is this command and the `gslb-service-port-cfg max` command and applies the limit with the lower value. For example, if `gslb-service-port-cfg max` is set to a limit of 10k and `slb resource-usage real-port-count` is set to a limit of 5k, the limit of 5k set in `real-port-count` is considered.
real-server-count	Total number of real servers (512-8192) in the system.

Resource Type	Description and Acceptable Values
	NOTE: GSLB resource limit considers the limit set is this command and the `gslb-service-ip-cfg max` command and applies the limit with the lower value. For example, if `gslb-service-ip-cfg max` is set to a limit of 10k and `slb resource-usage real-server-count` is set to a limit of 5k, the limit of 5k set in `real-server-count` is considered.
server-ssl-template-count	Total number of server SSL templates (32-8192) in the system.
service-group-count	Total number of service groups (512-8192) in the system.
stream-template-count	Total number of configurable streaming media templates (32-4096) in the system.
virtual-port-count	Total number of virtual ports (256-8192) in the system.
virtual-server-count	Total number of virtual servers (512-4096) in the system.
substitute-source-mac	Specifies that the client (source) MAC address of the packet sent to the load balancing server is replaced with the MAC address of the outgoing interface (for example, an ACOS device). This allows real servers in a load balancing environment to make web cache or security device responses to the source MAC of the ACOS device.

Default The default maximum number for each type of system resource depends on the specific device model. To display the defaults and current values for your device, enter the **show system resource-usage**

command for system level and **show slb resource-usage** command for slb level.

Mode Configuration mode

Usage These SLB resources are configurable at the system level and not limited to the partition level. The maximum number of resources you can configure depends on the resource type and the specific platform. To display the range of values that are valid for a resource, enter a question mark instead of a quantity.

- For these SLB templates, the maximum is 256 each, and is not configurable:
  - SIP
  - SMTP
  - Policy (PBSLB)
- For RAM caching templates, the total number allowed is 128 each.
- The maximum number of health monitors is 1024 (not configurable).
- The maximum number of wildcard VIPs per device is based on the system memory size, while the maximum wildcard VIP limit is 200 for per partition. For more information, see the 'Wildcard VIPs, Ports, and Virtual Ports' section in the *Application Delivery Controller Guide*.
- For every type of system resource that has a default, the ACOS device reserves one instance of the resource.

  For example, the device allows 256 RAM caching templates. However, the device reserves one RAM caching template for the default template, which leaves a maximum of 255 additional configurable RAM caching templates.

  The `substitute-source-mac` option is available at the slb virtual-server level. It replaces the source MAC of the client in a L2 setting at the global level.

Example

```
ACOS# slb common
ACOS(config-common)#  slb resource-usage substitute-source-mac
```

slb resource-usage threshold

Description Specifies the utilization percentage at which the device issues a log message and SNMP notification for SLB resources. The **slb resource-usage** command configures capacity of the SLB resources affect by this command.

Syntax

```
[no] slb resource-usage threshold percentage
```

The *percentage* specifies usage that triggers a log message and SNMP notification, as a percentage of resource capacity. Value range is 1 through 99.

Default 0% is applied

Mode Configuration mode

Example This example configures capacity maximums for virtual ports (2000) and virtual servers (400), then specifies the number of configured ports (1200) and servers (240) that triggers a log message and notification.

Example While this example explicitly demonstrates the threshold command affect on these two resources, it affects device behavior for all resources controlled by the **slb resource-usage** command

```
ACOS(config)# slb resource-usage virtual-port-count 2000
Changes will come into effect next time you reload the
Software.
ACOS(config)# slb resource-usage virtual-server-count 400
Changes will come into effect next time you reload the
Software.
ACOS(config)# slb resource-usage threshold 60
ACOS(config)#
```

slb server

Description Configure a real server. Use the first command shown below in the example to create or a delete a server. Use the second command to edit a server.

Syntax

```
[no] slb server server-name {ipaddr | hostname |use-aam-
server}
```

The “no” form of this command deletes the specified real server. If the **delete-referenced-tagged-objects** option of system config-mgmt is enabled, the default setting, the system deletes the real server regardless of any existing references. If this option is disabled, the system checks if the real server is being referenced by other objects and prevents deletion until all references are manually removed.

Parameter	Description
server-name	Specify the server name, 1-63 characters. If you want to rename the server name, then use **rename** global configuration command.
hostname	Specify the Fully-qualified hostname, for dynamic real server creation.
ipaddr	Specify the IP address of the server (IPv4 or IPv6). This is required only if you are creating a new server.
ethernet	Specify the ethernet interface. This must be an ethernet virtual wire endpoint or member of a virtual-wire-ethernet-group. If the server is selected, then the traffic will go out through the ethernet interface.
use-aam-server	Allow the SLB server to reuse the same AAM authentication server (IP address). The authentication server can be LDAP, OSCP, RADIUS, and Kerberos. Similarly, the IP can be the hostname, IPv4 address, or IPv6 address. **NOTE:** The real server is created after binding the authentication server to the authentication service group. Also, you must enable health check on the authentication server. For more information, see*Application Access Management guide*.

Default N/A

Mode Configuration mode

Usage This command creates a new or edits an existing real server and changes the CLI to the server configuration level.

A new real server is created, if required, by adding a server to a service group, obviating the need to explicitly create a real server prior to adding it to a group. The IP address of the server can be in either IPv4 or IPv6 format.

The maximum number of real servers is configurable under slb resource-usage.

Example The following example creates a new real server with an IPv4 address:

```
ACOS(config)# slb server rs1 10.10.10.99
ACOS(config-real server)#
```

Example The following example creates a new real server with an IPv6 address:

```
ACOS(config)# slb server rs2 2020:3e8::3
ACOS(config-real server)#
```

Example The following commands configure a hostname server for dynamic server creation using DNS, add a port to it, and bind the server template to it.

To create the *temp-server* template, use slb template server.

```
ACOS(config)# slb server s-test1 s1.test.com
ACOS(config-real server)# template server temp-server
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
```

Example The following example creates real server associating the ethernet interface:

```
ACOS(config)# slb server rs2 ethernet 2
ACOS(config-real server)# port 80 tcp
```

Example The following example allows SLB server to reuse the same AAM authentication server (IPv4 address):

```
ACOS(config)#slb server 192.168.90.136 use-aam-server
```

```
ACOS(config-real server)# port 389 tcp
```

support-http2

Description Start the HTTP/2 connection with prior knowledge and send HTTP/2 frames directly.

Syntax

```
[no] support-http2 {only}
```

Parameter	Description
support-http2	Specify this command in a real server if the server side supports HTTP/2. ACOS will send the HTTP/2 request with prior-knowledge to the server if the client request is HTTP/2. **NOTE:** The HTTP/1.1 to HTTP/2 upgrade mechanism will not be supported as specified in RFC 9113.
only	This is an optional parameter. Specify this option when the server side can only handle HTTP/2 traffic. This option should be enabled only when the HTTP/2 is configured on the server side. For more information, see HTTP/1.1 to HTTP/2 communication support section in *Application Delivery Controller Guide*.

Default Not enabled.

Mode SLB real server

Example The following command enables HTTP/2 support on real server.

```
ACOS(config)# slb server realserver1 10.1.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# support-http2
```

Related Commands:

- slb template http

alternate

Description Assign an alternate server as a dedicated backup for a primary server.

Syntax

```
[no] alternate sequence-num server-name
```

Parameter	Description
sequence-num	Priority of the server as a backup. You can specify 1-16.
server-name	Name of the alternate server.

Default Not set

Mode Real server

Usage You can assign up to 16 alternate servers to a primary server. Only 1 alternate server for a given primary server can be active at a time.

This feature places an alternate server into service *only* if the primary server goes down. Other features such as connection limiting or connection-rate limiting can not cause an alternate server to be used. Do not add alternate servers to the service group.

For more information, see the “Alternate Servers for Server-specific Backup” chapter in the *Application Delivery Controller Guide*.

conn-limit

Description Specify maximum number of concurrent connections allowed on a real server.

Syntax

```
[no] conn-limit max-connections
```

Replace *max-connections* with the maximum number of concurrent connections allowed on the server. You can specify 1-64000000 (64 million).

Default 64000000

Mode Real server

Usage If you set a connection limit, it is recommended that you also set the conn-resume interval. (See conn-resume.)

You also can set the connection limit (1-64000000) on individual protocol ports. In this case, the limit specified for the port overrides the limit set at the server level.

Example The following command sets the connection limit to 10,000:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# conn-limit 10000
```

conn-resume

Description Specify the maximum number of connections the server can have before the ACOS device resumes use of the server. Use does not resume until the number of connections reaches the configured maximum or less.

Syntax

```
[no] conn-resume connections
```

Replace *connections* with the maximum number of connections the server can have before the ACOS device resumes use of the server. You can specify 1-1000000 (1 million) connections.

Default By default, this option is not set. The ACOS device is allowed to start sending new connection requests to the server when the number of connections on the server falls below the connection limit threshold set by `conn-limit`.

Mode Real server

Usage You also can set the conn-resume value on individual protocol ports. In this case, the value specified for the port overrides the value set at the server level.

Example The following command sets the conn-resume option to 500,000 connections:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# conn-resume 500000
```

disable

Description Disable a real server.

Syntax

```
[no] disable
```

Default Enabled

Mode Real server

Example The following commands disable a server named “rs123”:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# disable
```

disable-with-health-check

Description Disable a service-group member from normal server selection, but still maintain the health of the server.

This feature is ideal if you periodically need to take active servers out of service pools for maintenance, but this maintenance is done through a remote client. The feature allows you to access these servers using the same front-end VIP in the presence of a persistent cookie template or `LB::reselect` aFleX command.

This feature is available in ACOS 4.0.1 and later.

Syntax

```
disable-with-health-check
```

Default This feature is not enabled be default.

Mode Real server

Usage In addition to real server configuration mode, this command is also available from the following modes:

- Real server port configuration (see port)
- Service -group member (see member)

Example This example configures health monitor “hm1” to use ICMP transparent health method and apply the monitor to a TCP port on real server “realserver1”. **`Disable-with-health-check`** is enabled at the SLB server configuration level.

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method icmp transparent 1.0.0.1
ACOS(config-health:monitor)# exit
ACOS(config)# slb server realserver1 10.1.1.2
ACOS(config-real server)# disable-with-health-check
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# health-check hm1
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg1 tcp
ACOS(config-slb svc group)# member realserver1 80
ACOS(config-slb svc group-member:80)#
```

enable

Description Re-enable a real server.

Syntax

```
[no] enable
```

Default Enabled

Mode Real server

Example The following commands re-enable a disabled server named “rs123”:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# enable
```

extended-stats

Description Enable collection of peak connection statistics for a server.

Syntax

```
[no] extended-stats
```

Default Disabled

Mode Real server

external-ip

Description Assign an external Network Address Translation (NAT) IP address to the server. The external IP address allows a server that has an internal IP address to be reached from outside the internal network.

Syntax `[no] external-ip ipaddr`

Default None

Mode Real server

Example The following commands configure external IP address 192.168.10.11 on real server “rs123”:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# external-ip 192.168.10.11
```

health-check

Description Enable health monitoring for a server.

Syntax `[no] health-check monitor-name`

Replace *monitor-name* with the name of a configured health monitor. If you omit this command, the default ICMP health monitor is used. (See below.)

Default ICMP ping (echo request), sent every 5 seconds. If ping fails 4 times consecutively (first attempt followed by 3 retries), ACOS device sets the server state to DOWN.

Mode Real server

Usage Entering the command at this level enables Layer 3 health checking. The monitor you specify must use the ICMP method.

Example The following command sets a server to use the “RUthere” health monitor:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# health-check RUthere
```

health-check-disable

Description Disable health monitoring of the server.

Syntax `[no] health-check-disable`

Default The default Layer 3 health method (ping) is used by default.

ipv6

Description Assign an IPv6 address to the real server for GSLB.

Syntax `[no] ipv6 ipv6addr`

Default None

Mode Real server

port

Description Configure a TCP or UDP port on a server.

Syntax `[no] port port-num {tcp | udp} [range | port-service-name num]`

Parameter	Description
port-num	Protocol port number, 0-65534. Port number 0 is a wildcard port used for IP protocol load balancing. For more information, see the "IP Protocol Load Balancing" chapter of the *Application Delivery Controller Guide*.
tcp | **udp**	Protocol type. When configuring a port for NetFlow, use UDP. TCP is not supported for NetFlow.
range *num*	Specifies the range of real ports you want to create within the real server configuration. This value can range from 0-254. The specified port number is the base number for the range of real ports.
port-service-name	Specify a label for a port service. Multiple services can be defined within a port for different applications, such as, HTTP or FTP. The length of the port service can range from 1-64 characters.

This command changes the CLI to the configuration level for the specified port service, where the following commands are available:

Command	Description
[**no**] **alternate** *sequence-num server-name* **port** *portnum*	Configure an alternate port for the primary port. *Sequence-num* and *server-name* can be 1-16. (For more information, see "Dedicated Backups for Real Server Ports" in the *Application Delivery Controller Guide*.)
[**no**] **authentication-server** *profile-name*	Binds an authentication-server profile to the port. **NOTE**: This option applies to Application Access Management (AAM).
[**no**] **conn-limit** *max-connections*	Specifies the maximum number of concurrent connections allowed on the server for this port, 1-64000000 (64 million). The default is 64000000.
[**no**] **conn-resume** *connections*	Specifies the maximum number of connections the service port can have before the ACOS device resumes use of the port. Use does not resume until the number of connections reaches the configured maximum or less. You can specify 1-1000000 (1 million) connections. By default, this option is not set. The ACOS device is allowed to start sending new connection requests to the service port as soon as the number of connections on the port falls back below the connection limit threshold set by the **conn-limit** command.
disable	Disables the port.
disable-with-health-check	Disable member service port, but maintain the server's health check status. This feature is introduced in ACOS 2.7.2-P2 and

Command	Description
	later, and ACOS 4.0.1 to allow you to disable a service-group member's port from normal server selection, but still maintain the health of the server. This feature is ideal if you periodically need to take active servers out of service pools for maintenance, but this maintenance is done through a remote client. The feature allows you to access these servers using the same front-end VIP in the presence of a persistent cookie template or `LB::reselect` aFleX command.
enable	Enables the port.
[**no**] **extended-stats**	Enables collection of SLB peak connection statistics for the port.
[**no**] **health-check** *monitor-name*	Enables health monitoring of the port service. The ***monitor-name*** specifies the name of a configured health monitor. If you omit this command or you enter it without the **monitor-name** option, the default TCP or UDP health monitor is used: • TCP – Every 5 seconds, the ACOS device sends a connection request (TCP SYN) to the specified TCP port on the server. The port passes the health check if the server replies to the ACOS device by sending a TCP SYN ACK. • UDP – Every 5 seconds, the ACOS device sends a packet with a valid UDP header and a garbage payload to the UDP port. The port passes the health check if the server either does not reply, or replies with any type of packet *except* an ICMP Error message.

Command	Description
[no] **health-check-follow-port** *port-num* {**tcp** | **udp**}	Specifies another real port upon which to base this port's health status. Both the real port and the port to use for the real port's health status must be the same type, TCP or UDP. By default, this option is not set.
[no] **health-check-disable**	Disables health monitoring of the port.
[no] **no-ssl**	Disables SSL for server-side connections. This command is useful if a server-SSL template is bound to the virtual port that uses this real port, and you want to disable encryption on this real port. Encryption is disabled by default, but it is enabled for server-side connections when the real port is used by a virtual port that is bound to a server-SSL template. Using the double-negative form of the command (**no no-ssl**) enables SSL for server-side connections.
[no] **service-principal-name** *string* [...]	Specifies the Kerberos principal name of this server port. This is the ACOS client name presented to the application server. **NOTE:** This option applies to Application Access Management (AAM).
stats-data-disable | **stats-data-enable**	Disable or enable statistical data collection for the port.
[no] **template port** *template-name*	The **port** option binds a port template to the port. The parameter settings in the template are applied to the port.

Command	Description
	The real port template named “default” is bound to real ports by default. Parameter settings in the default real port template automatically apply to the port, unless you bind a different real port template to the port. If a parameter is set individually on this port and also is set in a port template bound to this port, the individual setting on this port is used instead of the setting in the template. To configure a port template, see slb template port.
[**no**] **template server-ssl** *template-name*	The **server-ssl** option binds a server-side SSL template to the port. The parameter settings in the template are applied to the port. This is useful where the real servers load balanced by a VIP have different SSL settings.
[**no**] **weight** *number*	Specifies load-balancing preference for this port, 1-1000. Higher weights give more favor to this server for this port relative to other servers. Default is 1. This option applies only to the **service-weighted-least-connection** load-balancing method.

Default No ports are configured by default. The defaults for the command options are described with the options, above. Statistical data collection of load-balancing resources is enabled by default.

Mode Real server

The **no** form of this command resets the port’s connection limit, health monitoring, or weight to its default value. To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally.

Usage Include the **range** option for each real server that will be included in the service group, but only if you want that real server to be included in the mapping feature. The service group can be "mixed". That is, some real servers within a service group can have the range option set, but it is not mandatory for all servers in a service group to be configured for "VIP to real port mapping".

Example The following commands configure server "terap" and add TCP port 69 to the server. The **health-check** command is not entered, so by default the ACOS device will check the service port's health by sending a connection request to 69 on terap every 30 seconds.

```
ACOS(config)# slb server terap 10.2.4.69
ACOS(config-real server)# port 69 tcp
ACOS(config-real server-node port)#
```

Example The following commands bind the server-SSL template directly to TCP port 80 on the real server at IP 10.8.8.8:

```
ACOS(config)# slb server rs88 10.8.8.8
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# template server-ssl
server-ssl1
```

Example The following example configures health monitor "hm1" to use the ICMP transparent health method, and apply the monitor to a TCP port on real server "realserver1". The **disable-with-health-check** option is enabled at the SLB server port configuration level.

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method icmp transparent 1.0.0.1
ACOS(config-health:monitor)# exit
ACOS(config)# slb server realserver1 10.1.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# health-check hm1
ACOS(config-real server-node port)# disable-with-health-check
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg1 tcp
ACOS(config-slb svc group)# member realserver1 80
ACOS(config-slb svc group-member:80)#
```

Example The following commands configure the 'http and 'gitlab' labels for port services under base port 80.

```
ACOS(config)# slb server slb1 10.10.10.20
ACOS(config-real server)# port 80 tcp http
ACOS(config-real server-node port)# exit
ACOS(config-real server)# port 80 tcp gitlab
ACOS(config-real server-node port)# exit
```

slow-start

Description Enable slow-start for a server. Slow start allows time for a server to ramp up after the server is enabled or comes online, by temporarily limiting the number of new connections on the server.

It is recommended to configure this feature in the real server template or real port template instead. See the “Behavior When Slow Start Is Also Configured on the Real Server Itself” section in the “Server and Port Templates” chapter of the *Application Delivery* **Controller** *Guide*.

Syntax

```
[no] slow-start
```

Default Disabled

Mode Real server

Usage Slow-start allows a maximum of 128 new connections during the first interval (anywhere between 0 and 10 seconds). During each subsequent 10-second interval, the total number of concurrent connections allowed to the server is doubled. Thus, during the first 20 seconds, the server is allowed to have a total of 256 concurrent connections. After 59 seconds, slow-start ends the ramp-up and no longer limits the number of concurrent connections.

After the ramp-up period ends, the number of new connections is controlled by the conn-limit setting. (See clear slb virtual-server and the description of conn-limit in port.)

Slow-start is also configurable in slb template server and slb template port.

Example The following command enables slow-start:

```
ACOS(config)# slb server rs123
ACOS(config-real server)# slow-start
```

spoofing-cache

Description Enable support for a spoofing cache server. A spoofing cache server uses the client's IP address instead of its own as the source address when obtaining content requested by the client.

Syntax

```
[no] spoofing-cache
```

Default Disabled

Mode Real server

Usage This command applies to the Transparent Cache Switching (TCS) feature. For more information about TCS, including additional configuration requirements and examples, see the "Transparent Cache Switching" chapter in the *Application Delivery Controller Guide*.

Example The following commands configure a real server for a spoofing cache server:

```
ACOS(config)# slb server cache-rs 110.110.110.10
ACOS(config-real server)# spoofing-cache
ACOS(config-real server)# port 80 tcp
```

stats-data-disable

Description Disable collection of statistical data for the server.

Syntax

```
stats-data-disable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Real server

stats-data-enable

Description Enable collection of statistical data for the server.

Syntax

```
stats-data-enable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Real server

Usage To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally. (See slb common.)

template server

Description Bind a real server template to the server.

Syntax

```
[no] template server template-name
```

Default The real server template named “default” is bound to servers by default. The parameter settings in the default real server template are automatically applied to the new server, unless you bind a different real server template to the server.

Mode Real server

Usage If a parameter is set individually on this server and also is set in a server template bound to this server, the individual setting on this server is used instead of the setting in the template.

To configure a real server template, see slb template server.

Example The following commands configure a real server template called “rs-tmplt1” and bind the template to two real servers:

```
ACOS(config)# slb template server rs-tmplt1
ACOS(config-rserver)# health-check ping2
ACOS(config-rserver)# conn-limit 500000
ACOS(config-rserver)# exit
ACOS(config)# slb server rs1 10.1.1.99
ACOS(config-real server)# template server rs-tmplt1
ACOS(config-real server)# exit
ACOS(config)# slb server rs2 10.1.1.100
ACOS(config-real server)# template server rs-tmplt1
```

weight

Description Assign an administrative weight to the server, for weighted load balancing.

Syntax

```
[no]  weight  num
```

Replace *num* with the administrative weight assigned to the server. You can specify 1-1000.

Default 1

Mode Real server

Usage This parameter applies only to the **weighted-least-connection**, **weighted-rr** (weighted round robin), and **round-robin-strict** load-balancing methods.

Example The following commands assign a weight of 20 to a server:

```
ACOS(config)# slb server 10.10.10.5
ACOS(config-real server)# weight 20
```

slb service-group

Description Configure an SLB service group.

Syntax

```
[no]slb service-group group-name {tcp | udp}
```

The “no” form of this command deletes the specified service group. If the **delete-referenced-tagged-objects** option of system config-mgmt is enabled (the default setting), the system deletes the service group regardless of any existing references. If this option is disabled, the system checks if the service group is being referenced by other objects and prevents deletion until all references are manually removed.

Parameter	Description
group-name	Name of the group, 1-127 characters. If you want to rename the server name, then use

Parameter	Description
	rename global configuration command.
tcp | **udp**	Application type of the group.

Default There are no service groups configured by default.

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing service group. The CLI changes to the configuration level for the service group.

Example The following example adds TCP service group “my-service-group”:

```
ACOS(config)# slb service-group my-service-group tcp
ACOS(config-slb svc group)#
```

backup-server-event-log

Description Enable log messages to indicate when a backup service-group member is placed into service or is removed from service.

Syntax

```
[no] backup-server-event-log
```

Default Disabled

Mode Service group

A *backup* member is a member that has a lower priority than primary (highest priority) members of the same service group. The ACOS device will not use a lower-priority member (backup server) unless high priority members (primary servers) exceed their connection limits or connection-rate limits, or are down.

The **backup-server-event-log** command generates a log message when a backup service-group member is placed into service for either of these reasons:

- The connection limit on the primary servers or member ports is exceeded.
- The primary servers or member ports go down.

Likewise, the command generates a log message when a backup service-group member is removed from service, and a primary server is returned to service for either of the following reasons:

- The primary server or member port's connection-resume limit is reached.
- The primary server or member port comes back up.

Generation of log messages for these events is rate-limited to once per minute. The events described in a message occur at some point within the 60 seconds prior to the log message's timestamp.

By default, the backup servers are placed into service only when both primary servers exceed their connection limits or go down. You can use the **min-active-member** command to allow secondary servers to be placed into service even when some primary servers are still available. (See min-active-member.)

SNMP Trap Requirements

To also generate SNMP notifications, the following SLB traps must be enabled:

- slb server-conn-limit
- slb server-conn-resume
- slb service-conn-limit
- slb service-conn-resume

Log Message Examples

A message such as the following is generated when a backup member is placed into service:

```
Enabled new connections on server rs-backup1 port 80 in sg1
group
```

In this example, member *rs-backup1* in service group *sg1* is placed into service.

When the backup member is removed from service, a message such as one of the following is generated:

```
Disabled new connections on backup server(s) on group sg1,
resume primary server rs1 port 80
```

```
Disabled new connections on backup server(s), resume primary
server rs1 port 80
```

In the first message, the service group name is included. The service group name is not included in the second message.

- If the primary server is a member of only one service group, or the service group can otherwise be determined, the first message is used.
- If the primary server is a member of more than one service group, and the service group can not be determined, the second message is used.

extended-stats

Description Enable collection of peak connection statistics for a service group.

Syntax

```
[no] extended-stats
```

Default Disabled

Mode Service group

health-check

Description Enables health monitor to check the health of all members of the service group.

Syntax

```
health-check monitor-name
```

Replace *monitor-name* with with the name of a configured health monitor. If you omit this command, the default ICMP health monitor is used.

Default ICMP ping (echo request), sent every 5 seconds. If ping fails 4 times consecutively (first attempt followed by 3 retries), ACOS device sets the server state to DOWN.

Mode Service group

Usage The health monitor is used to test the health of all members of the service group, including any members that are added in the future.

Service group health status applies only within the service group context. Health checks of a port from different service groups can result in different health status, depending on the resource requested by the health check.

Health checks can be applied to the same resource (real server or port) at the following levels:

- In a service group that contains the server and port as a member
- In a server or server port configuration template bound to the server or port
- Directly on the individual server or port

In cases where health checks are applied at multiple levels, they have the following priority:

1. Health check on real server
2. Health check on real server's port
3. Health check on service group

If a health check at the real server level (1) fails, the corresponding real server, real server port, and service group members are marked Down. However, if a health check on the service group level (3) fails, only that service group member in that service group is marked Down.

Example These commands configure a health monitor and apply it to a service group:

```
ACOS(config)# health monitor qrs
ACOS(config-health:monitor)# method http url GET /media-qrs/index.html
ACOS(config-health:monitor)# exit
ACOS(config)# slb service-group qrs tcp
ACOS(config-slb svc group)# member media-rs 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# health-check qrs
```

health-check-disable

Description Disable health monitoring of the service group.

Syntax

```
[no] health-check-disable
```

Default Health checking is enabled by default.

member

Description Add a server to a service group.

Syntax

```
[no] member server-name portnum
```

Parameter	Description
server-name portnum	Name of the real server you want to add to the service group. This server must already exist on the

Parameter	Description
	system.
portnum	Protocol port number on the server.

This command drops you into a sub-configuration mode, where the following additional commands are available:

Parameter	Description
enable	Enable the server and port for this service-group only.
disable	Disable the server and port for this service-group only.
disable-with-health-check	Disable the member server, but maintain the server's health check status. This feature is introduced in ACOS 2.7.2-P2 and later, and ACOS 4.0.1 to allow you to disable a service-group member from normal server selection, but still maintain the health of the server. This feature is ideal if you periodically need to take active servers out of service pools for maintenance, but this maintenance is done through a remote client. The feature allows you to access these servers using the same front-end VIP in the presence of a persistent cookie template or `LB::reselect` aFleX command.
priority *num*	Sets the preference for this server and port, 1-16. The highest priority is 16.
sampling-enable *param*	Enable baselining. The following parameters are available: • all - All connections. • curr_conn - Current connections. • total_fwd_bytes - Total forward bytes. • total_fwd_pkts - Total forward packets. • total_rev_bytes - Total reverse bytes. • total_rev_pkts - Total reverse packets.

Parameter	Description
	• total_conn - Total connections. • total_rev_pkts_inspected - Total reverse packets inspected. • total_rev_pkts_inspected_status_code_2xx - Total reverse packets inspected (status code 2xx). • total_rev_pkts_inspected_status_code_non_5xx - Total reverse packets inspected (status code non 5xx). • curr_req - Current requests. • total_req - Total requests. • total_req_succ - Total requests successful. • peak_conn - Peak connections. • response_time - Response time. • fastest_rsp_time - Fastest response time. • slowest_rsp_time - Slowest response time.
stats-data-disable	Disable statistical data collection for the service-group member.
template *template-name*	Binds a real port template to this member port. **NOTE:** The port template option **slow-start** is not supported if the port template is applied using this command.
stats-data-disable	Disable statistical data collection for the service-group member.

Default There are no servers in a service group by default. When you add a server and port to the service group, the default state is enabled and the default priority is 1. Statistical data collection of load-balancing resources is enabled by default.

To configure a real port template, see slb template port.

Mode Service group

Usage The normal form of this command adds a configured server to the service group. The “no” form of this command removes the server from the group.

If you disable or re-enable a port, the state change applies only to this service group. The state of the port is unchanged in other service groups.

To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally.

Example The following commands add servers “s1” and “s2” to service group “sgroup1”:

```
ACOS(config)# slb service-group sgroup1
ACOS(config-slb svc group)# member s1 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s2 80
ACOS(config-slb svc group-member:80)# exit
```

Example The following command adds a member server and port to a service group and binds a real port template to the port:

```
ACOS(config)# slb service-group sg1 tcp
ACOS(config-slb svc group)# member rs1 80
ACOS(config-slb svc group-member:80)# template rptemplate1
```

Example The following example configures health monitor “hm1” to use the ICMP transparent health method, and apply the monitor to a TCP port on real server “realserver1”. Then, the **disable-with-health-check** option is enabled at the service group member configuration level.

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method icmp transparent 1.0.0.1
ACOS(config-health:monitor)# exit
ACOS(config)# slb server realserver1 10.1.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# health-check hm1
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg1 tcp
```

```
ACOS(config-slb svc group)# member realserver1 80
ACOS(config-slb svc group-member:80)# disable-with-health-
check
```

method

Description The method command is a service-group configuration mode command that specifies the load balance method used to determine which server receives an inbound data flow (session). After a server is selected for a session, that server receives packets from the session until the timeout expiry, defined as the period of time the load balancer does not receive at least one packet of the session.

The default timeout period is 180 seconds.

A session is defined by its five-tuple: source IP address, source port, destination IP address, destination port, and protocol. Each selection option utilizes at least one of the following four data points:

- session packet contents (typically destination IP address and port)
- load balancer configuration parameters (typically weight settings)
- health monitor packets received from member servers
- metrics managed by load balancers (such as number of connections sent to each server)

Syntax

```
[no]  method lb-method
[auto-switch
  [
  stateless-lb-method
     {
     conn-rate rate duration
       [revert-rate revert-duration]
         [grace-period seconds] [log] |
     l4-session-usage percent duration
       [revert-rate revert-duration]
         [grace-period seconds] [log]
  ]
    } ]
```

Parameter	Description
lb-method	Load-balancing method: • **dest-ip-hash** – Calculates a hash value based on

Parameter	Description
	the destination IP address and protocol port of the client's request. • **dest-ip-only-hash** – Calculates a hash value based on only the destination IP address of the client's request. • **fastest-response** – Selects the server with the fastest first data packet response time (after three-way handshake) from end-user traffic requests. The **fastest-response** method is not applicable in Direct Server Return (DSR) deployments. • **least-request**– Selects the real server port for which the ACOS device is currently processing the fewest HTTP requests. • **weighted-least-request**– Selects the real server based on the formula **least request count/server weight** and accordingly selects the server with the minimum value for load balancing. • **service-weighted-least-request**– Selects the service port based on the formula **least request count/port weight** and accordingly selects the service port with the minimum value for load balancing. • **src-ip-hash** – Calculates a hash value based on the source IP address and protocol port of the client's request. • **src-ip-only-hash** – Calculates a hash value based on only the source IP address of the client's request. • **weighted-rr**– Selects servers in rotation, based on the servers' administratively assigned weights. To use this method, you also need to assign weights to the servers. (See weight.) If the weight value is the

Parameter	Description
	same on each server, this load-balancing method simply selects the servers in rotation. The **weighted-rr** method uses only the server weight. Server port weight is not used. (Instead, server port weight is used by the **service-weighted-least-connection** method). **NOTE:** For performance optimization, ACOS may distribute traffic based on per data CPU view instead of a global view. Over extended periods, the traffic will be distributed evenly across all servers, ensuring balanced performance. • **weighted-rr-interleave** – Selects servers in an interleaved rotation based on the administratively assigned weights. The client requests are distributed among servers sequentially, regardless of whether the previous server's weight has been exhausted. The weight is evenly distributed across all CPUs of the server. This prevents the magnification of the excess weight by the total number of CPUs. This method mitigates connection bursts and minimizes the accumulation of unused connections in the reuse queue. **NOTE:** This method cannot be used with a service group member having a priority value set. • **service-weighted-rr** – Provides weighted round robin at the server port level. • **round-robin** – Selects servers in simple rotation. • **round-robin-strict** – Provides a more exact round-

Parameter	Description
	robin method. The standard, default round robin method is optimized for high performance. Over time, this optimization can result in a slight imbalance in server selection. Server selection is still basically round robin, but over time some servers may be selected slightly more often than others. An optional weight can also be assigned. (See weight.) These methods apply only to stateless SLB. See the "Usage" section for more information. • **odd-even-hash** – Hash value is even-odd result of the sum of the source IP address octets. • **service-least-request-pseudo-round-robin** – This method performs two levels of comparison to select the service group: ◦ At the first level, it selects the server that has the least number of unanswered requests. ◦ If two servers have the same number of unanswered requests, the pseudo-round-robin act as the second level. It chooses the server that has not been selected for the longest time, as per its timestamp. • **least-connection** [**pseudo-round-robin**] – Selects the server that currently has the fewest connections. For this and the other least-connection methods, if there is a tie, the default behavior is to select the port (among those tied) that has the lowest number of request bytes plus response bytes. If there is still a tie, a port is randomly selected from among the ones that are still tied. To override this tie-breaker behavior, use the **pseudo-round-robin** option. This option selects the

Parameter	Description
	server that has not been selected for the longest time. • **link-cost-load-balance** – In this method, link usage is prioritized based on the cost of the bandwidth for the connection. If the link utilization exceeds the pre-configured bandwidth, then the excess traffic is sent to the link operating at the lowest overage cost. Additionally, in case of link failure, traffic is sent to the next available link. **Note:** ◦ Each link can only be referenced by one tcp service-group and one udp service-group. ◦ When a node is bound to a link-cost service-group, it becomes a link cost node. It is not allowed to bind to another method type. ◦ Maximum of 16 nodes are allowed per service group. • **service-least-connection** [**pseudo-round-robin**] – Selects the server port that currently has the fewest connections. • **weighted-least-connection** [**pseudo-round-robin**] – Selects a server based on a combination of the server's administratively assigned weight and the number of connections on the server. (To assign a weight to a server, see weight.) • **service-weighted-least-connection** [**pseudo-round-robin**] – Same as **weighted-least-connection**, but per service. (To assign a weight to a service, see port. Use the **weight** option.)
lb-method (cont.)	Load balancing method (continued):

Parameter	Description
	• **stateless-src-ip-hash** – Balances server load based on a hash value calculated using the source IP address and source TCP or UDP port. • **stateless-src-dst-ip-hash** – Balances server load based on a hash value calculated using both the source and destination IP addresses, and the source and destination TCP or UDP ports. • **stateless-src-dst-ip-only-hash** – Balances server load based on a hash value calculated using only the source and destination IP addresses. • **stateless-dst-ip-hash** – Balances server load based on a hash value calculated using the destination IP address and destination TCP or UDP port. • **stateless-per-pkt-round-robin** – Balances server load by sending each packet to a different server, in rotation. This method is applicable *only* for UDP DNS traffic. • **stateless-src-ip-only-hash** – Calculates a hash value based only on the source IP address of the request, and selects a server based on the hash value. Subsequently, all requests from the same client address are sent to the same server. • **stateless-per-pkt-weighted-rr** - Balances server load based on weight of each server, in rotation. This method is applicable only for traffic that uses a single packet for a request on server level. • **stateless-per-pkt-service-weighted-rr** - Balances server load based on weight of each service port, in rotation. This method is applicable *only* for traffic that uses a single packet for a request on service port level.
auto-	You can configure the following options for this feature.

Parameter	Description
switch *[options]*	The *stateless-lb-method* option specifies the stateless load-balancing method to use if the traffic reaches the configured threshold, and can be one of the following: • **stateless-dst-ip-hash** • **stateless-per-pkt-round-robin** • **stateless-src-dst-ip-hash** • **stateless-src-dst-ip-only-hash** • **stateless-src-ip-hash** • **stateless-src-ip-only-hash** • **stateless-per-pkt-weighted-rr** • **stateless-per-pkt-service-weighted-rr** You can specify either of the following sets of thresholds: • **conn-rate rate duration** – Rate of new connection requests per second at which the load balancing method is changed. The rate applies collectively to all servers in the service group. The threshold can be 1-1000000 connection requests per second. • **l4-session-usage** *percent duration* – Percentage of the system-wide Layer 4 session capacity that is currently in use. The threshold can be 1-100 percent. For each set of thresholds, you can specify the following options: • *revert-rate* – (Optional) Rate to revert to stateful method. You can specify 1-1000000 connections per second.

Parameter	Description
	Note: If no revert rate is specified, load balancing will remain stateless. For a switch to stateful to occur, a revert rate must be specified. • *revert-duration* – (Optional) Number of seconds during which the specified revert trigger must continue to occur before the service group changes to stateful load balancing again. You can specify 1-600 seconds. • **grace-period** *seconds* – (Optional) Number of seconds the ACOS device continues to use the current load balancing method for active sessions, before changing to the other load balancing method. You can specify 1-600 seconds. **NOTE**: The grace period applies only to sessions that are active when the load balancing change is triggered. The change applies immediately to new sessions that begin after the change is triggered. • **log** – Logs changes between stateful and stateless load balancing that occur due to this feature. This is disabled by default.

Default The default method is **round-robin**.

Mode Service group

Usage The **fastest-response** method takes effect only if the traffic rate on the servers is at least 5 connections per second (per server). If the traffic rate is lower, the first server in the service group usually is selected.

To set a server's weight, see weight.

Stateless SLB

Stateless SLB conserves system resources by operating without session table entries on the ACOS device. The stateless SLB methods are valid for the following types of traffic:

- Traffic with very short-lived sessions, such as DNS
- Layer 2 Direct Server Return (DSR) traffic
- Other types of traffic that do not require features that use session-table entries. (See list of limitations below.)

You can enable stateless SLB on an individual service-group basis, by selecting a stateless SLB load-balancing method for the group.

Limitations

- Stateless SLB is *not* valid for the following features or traffic types:
    - Rate limiting
    - ACLs
    - IP source NAT
    - Session synchronization
    - Application Layer Gateway (ALG)
    - Layer 3 DSR
    - SLB-PT
    - aFleX
    - FWLB ALG
- The following methods are all applicable to HTTP and HTTPS load balancing only:
    - least-request
    - weighted-least-request
    - service-weighted-least-request
    - service-least-request-pseudo-round-robin
- A given real server can be used in only one stateless SLB service group. A real server that is in a stateless SLB service group cannot be used in any other stateless service groups.
- If the virtual port is on a wildcard VIP, destination NAT must be disabled on the virtual port. To disable destination NAT, see no-dest-nat.

- Graceful transitions between stateful and stateless SLB in a service group are not supported.
- Mega-proxies may interfere with equal balancing of traffic load among the multiple data CPUs. In this case, for DNS traffic only, try using the stateless-per-pkt-round-robin method.

NOTE: The **stateless-per-pkt-round-robin** method is applicable only for traffic that uses a single packet for a request. Examples include DNS queries or RADIUS requests without a Challenge-request/Response message used for EAP.

Example The following commands configure stateless server load balance for weighted round-robin method. This method is similar to **stateless-per-pkt-round-robin** method and applicable only for traffic that uses a single packet for a request on server and service port level.

```
ACOS(config)# slb service-group sg-lvl udp
ACOS(config-slb svc group)# method stateless-per-pkt-weighted-rr
ACOS(config-slb svc group)# method stateless-per-pkt-service-weighted-rr
```

Example The following example sets the load-balancing method for a service group to least-connection:

```
ACOS(config)# slb service-group sg-lc1 tcp
ACOS(config-slb svc group)#  method least-connection
```

Example The following commands configure a stateless SLB service group for UDP traffic:

```
ACOS(config)#  slb service-group dns-stateless udp
ACOS(config-slb svc group)# member dns1 53
ACOS(config-slb svc group-member:53)# exit
ACOS(config-slb svc group)# member dns2 53
ACOS(config-slb svc group-member:53)# exit
ACOS(config-slb svc group)# method stateless-src-dst-ip-hash
```

Example The following commands configure a service group that uses the stateless-per-pkt-round-robin stateless load-balancing method. This method is used if the rate of new connection requests to the virtual

port bound to the service group reaches 80,000 connections per second, and remains at least this high for 300 seconds.

```
ACOS(config)# slb service-group auto-stateless tcp
ACOS(config-slb svc group)# method weighted-rr auto-switch
stateless-per-pkt-round-robin conn-rate 80000 300 60000 300
grace-period 15 log
```

To return to using the stateful load-balancing method (weighted round-robin in this example), the rate of new connection requests to the virtual port must drop to 60,000 per second, and remain that low for at least 300 seconds. Once this occurs, the ACOS device waits for and additional 15 seconds (the grace period) before returning to use of stateful load balancing. Logging is enabled.

Similarly, configure a service group that for other stateless load-balancing method.

Example

In the following configuration, if Layer 4 session usage reaches 2 percent and stays at least this high for 5 seconds, both service-group members begin using the stateless-dst-ip-hash method. The ACOS device reverts back to stateful load balancing when 1 percent or less is reached for 5 seconds.

```
ACOS(config)# slb service-group sg-auto1 tcp
ACOS(config-slb svc group)# method dst-ip-hash auto-switch
stateless-dst-ip-hash l4-session-usage 2 5 1 5
ACOS(config-slb svc group)# member s1 80
ACOS(config-slb svc group-member:80)# member s2 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb service-group sg-auto tcp
ACOS(config-slb svc group)# method dst-ip-hash auto-switch
stateless-dst-ip-hash l4-session-usage 2 5 1 5
ACOS(config-slb svc group)# member s3 80
ACOS(config-slb svc group-member:80)# member s4 80
```

min-active-member

Description

Use backup servers even if some primary servers are still up.

Syntax

```
[no] min-active-member num [dynamic-priority] [skip-pri-set]
```

Parameter	Description
num	Minimum number of primary servers that can still be active (available), before the backup servers are used. You can specify 1-63. There is no default.
dynamic-priority	Dynamically adds lower-priority servers to the active list to meet the min-active member requirement.
skip-pri-set	Specifies whether the remaining primary servers continue to be used. If you use this option, the ACOS device uses only the backup servers and stops using any of the primary servers.

Default By default, the servers with the highest priority value are the primary servers. All other servers are backups only, and are used only if all the primary servers are unavailable.

When you use this command, the **skip-pri-set** option is disabled by default.

Mode Service group

Usage Primary and backup servers are designated based on member priority (set with the **member** command). For example, if a service group contains real servers with the following priority settings, real servers s1, s2, and s3 are the primary servers. Real servers s4 and s5 are backup servers.

- s1 – priority 16
- s2 – priority 16
- s3 – priority 16
- s4 – priority 8
- s5 – priority 8

When the minimum number of active members (primary servers) comes back up, the ACOS device immediately returns to using only the primary servers.

Example The following commands add members with different priorities to a service group, and configure promiscuous VIP to begin using backup servers if any of the primary servers becomes unavailable:

```
ACOS(config)# slb service-group sg-prom tcp
```

```
ACOS(config-slb svc group)# method least-connection
ACOS(config-slb svc group)# member s1 80
ACOS(config-slb svc group-member:80)# priority 16
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s2 80
ACOS(config-slb svc group-member:80)# priority 16
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s3 80
ACOS(config-slb svc group-member:80)# priority 16
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s4 80
ACOS(config-slb svc group-member:80)# priority 8
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s5 80
ACOS(config-slb svc group-member:80)# priority 8
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb service group)# min-active-member 1
```

persist-scoring

Description Enables or Disables persist scoring at the service group level.

Syntax

```
[no] persist-scoring [global | enable | disable]
```

Parameter	Description
global	Use persists scoring set globally. **NOTE:** By default, the persist scoring is enabled globally. If the disable-persist-scoring command is configured under SLB common, this command will set the global configuration to default.
enable	Enables persist scoring only for the service group. It overrides the global configuration.
disable	Disables persist scoring only for the service group. It overrides the global configuration.

Mode SLB Service group

Example The following commands disable persist scoring at the service group level. The internal server selection in the service group will be based on the configuration:

```
ACOS(config)# slb service-group
ACOS(config-common)# persist-scoring disable
```

priority

Description Configure the ACOS device to respond to the failure of service-group members of a certain priority by taking a designated action, such as dropping the request or sending a TCP reset back to the client.

Syntax

```
priority num
[
  drop |
  drop-if-exceed-limit |
  proceed |
  reset |
  reset-if-exceed-limit
]
```

Parameter	Description
num	Priority of the port, ranging from 1-16. Higher-priority nodes are preferred over nodes with lower numbers. There is no default.
drop	Drops the request if all nodes with this same priority fail for any reason.
drop-if-exceed-limit	Drops the request if all nodes with this same priority fail, and if one or more nodes exceed the configured connection limit or connection-rate-limit.
proceed	The ACOS device uses the node(s) with the next-highest priority if all nodes with the currently-selected priority fail (this is the default behavior).
reset	Sends a reset to the client if all nodes with this same priority fail for any reason.
reset-if-exceed-limit	Sends a reset to client if all nodes with this same priority fail and if failure is due to one or more nodes exceeding configured connection-limit or connection-rate-limit.

Default By default, the ACOS device will use the node(s) with the next-highest priority if all nodes with the currently-selected priority fail.

Mode Service group

Usage Use this feature to define specific actions that should occur when higher-priority service-group members fail. By default, the ACOS device uses the highest priority service-group members until they are no longer available. When the higher-priority nodes fail, the device fails over to the nodes with the next-highest priority.

This priority option enables you to tie actions (drop, reset, and others) to a general failure, such as service group members becoming disabled or failing a health check. Alternatively, actions can be tied to connection-limits or connection-rate-limits being exceeded.

Configuring the "priority option" feature allows you to prevent lower-priority servers, which are presumably less robust than higher-priority servers, from being overwhelmed by a flood of traffic when a failover occurs.

NOTE: The actions are mutually exclusive. Only one action can be configured for each priority level.

The **reset** or **drop** actions can be triggered for the following reasons:

- If a health check fails
- If a user disables a server or port
- If another Load Balancing feature causes the currently-used priority to become unavailable (for example, **min-active-member** feature)
- If a connection-limit or connection-rate-limit is exceeded

Example The following commands create the TCP service group “sg1” with several servers with a priority of 10, and one server with a priority of 5. The commands also assign the **reset-if-exceed-limit** action for members with priority 10, and assign the **drop** action for members with priority 5.

```
ACOS(config)# slb service-group sg1 tcp
ACOS(config-slb svc group)# priority 10 reset-if-exceed-limit
```

```
ACOS(config-slb svc group)# priority 5 drop
ACOS(config-slb svc group)# member s1 80
ACOS(config-slb svc group-member:80)# priority 10
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s2 80
ACOS(config-slb svc group-member:80)# priority 10
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s3 80
ACOS(config-slb svc group-member:80)# priority 10
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s4 80
ACOS(config-slb svc group-member:80)# priority 5
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)#
```

priority-affinity

Description Configure the ACOS device to continue using backup servers (servers with lower priority) even when the primary (high priority) servers come back up.

Syntax

```
[no] priority-affinity [reset]
```

The **reset** option resets the priority affinity feature so that the primary servers can be used again.

Default Disabled.

By default, the ACOS device uses only the service-group members with the highest priority. If all the highest-priority servers go down, the ACOS device starts using the secondary (lower-priority) members. Also by default, when one or more of the highest-priority servers comes back up, the ACOS device returns to using only those highest-priority servers and stops using the backup servers.

Mode Service group

Usage The **min-active-member** option continues using backup servers in order to maintain a minimum number of active servers, but does not continue using only the backup servers after the primary servers come back up.

If the ACOS device stops using primary servers due to other features (such as exceeding connection limits), priority affinity takes effect just as if the switchover to the backup servers were triggered by a change in the status of the primary servers. If those higher-priority servers become available due to the number of connections dropping below the configured threshold, ACOS will not use them, but will instead continue using the lower-priority backup servers.

reset auto-switch

Description Reset load balancing from stateless back to the configured stateful method.

This command applies to configurations using auto-switch, which automatically switches from the configured stateful load-balancing method to a stateless load-balancing method, based on a configured threshold.

Syntax

```
reset auto-switch
```

Default N/A

Mode Configuration

Usage This command is operational only and does not affect the configuration. The command is not saved in the startup-config.

reset-on-server-selection-fail

Description Send a TCP reset (RST) to the client if server selection fails.

Syntax

```
[no] reset-on-server-selection-fail
```

Default Disabled

Mode Service group

sample-rsp-time

Description View sample server response time information.

Syntax

```
[no] sample-rsp-time [
  rpt-ext-server
```

```
  [report-delay mins | top-fastest | top-slowest]
]
```

Parameter	Description
rpt-ext-server	Report the top 10 fastest or slowest servers.
report-delay *mins*	Set the reporting frequency in minutes (1-7200).
top-fastest	Report the top 10 fastest servers.
top-slowest	Report the top 10 slowest servers.

Mode Service group

stats-data-disable

Description Disable collection of statistical data for the service group.

Syntax

```
stats-data-disable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Service group

stats-data-enable

Description Enable collection of statistical data for the service group.

Syntax

```
stats-data-enable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Service group

Usage To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally. (See slb common.)

strict-select

Description ACOS load balancing methods optimize for high performance, but sometimes this creates an imbalance in server selection, and some servers may have more open connections than others. For the round-

robin method of load balancing, the imbalances can be corrected when the option of “strict” is selected to ensure an exact round-robin distribution.

This method is supported for the Weighted Round-Robin, Least Connection, and Service Least Connection load balancing methods, guaranteeing that new connections will be sent to the server with the fewest connections, or fewest service connections. While strict load balancing can be configured with other load balancing methods, there will be no effect. Strict load balancing is enabled within a service-group configuration. When strict load balancing is enabled, lower performance should be expected, especially when ACOS is running a heavy load of traffic.

Syntax

```
[no] strict-select
```

Default Disabled.

Mode Service group

Example The following example configures a TCP load balancing service-group named “strict.” Within the service-group, the example configures least connection load balancing, and then enables strict selection.

```
ACOS(config)# slb service-group strict tcp
ACOS(config-slb svc group)# method weight-rr
ACOS(config-slb svc group)# strict-select
```

template

Description Apply a server or port configuration template to a service group.

Syntax

```
template
{policy template-name | port template-name | server template-
name}
```

Parameter	Description
policy *template-name*	Name of a policy template.
port *template-name*	Name of a port template.
server *template-name*	Name of a server template.

Default The settings in the server or port template applied to the server or port are used, unless overridden by settings in the individual server or port configuration.

Mode Service group

traffic-replication-type

Description Replicate or “mirror” traffic to one or more collector servers in a service group using one of the traffic replication types.

Syntax

```
traffic-replication-type {
 mirror |
 mirror-da-repl |
 mirror-ip-repl |
 mirror-sa-da-repl |
 mirror-sa-repl
}
```

Parameter	Description
mirror	The ACOS device sends the packets “as is” to the collector server(s). Forwarding is based on the IP address in the original packet. This mode does not change the packet header at all. The original Layer 2 Destination Address (DA) or Source Address (SA) and Layer 3 IP addresses are left intact.
mirror-da-repl	Mirror Destination MAC Address replacement mode uses Layer 2 forwarding, with the ACOS device replacing the destination MAC address on the incoming packet with the destination MAC for each of the collector servers within the designated service group.
mirror-ip-repl	Mirror IP-replacement mode replaces the incoming packet’s IP address with the IP address of the collector server(s) and then forwards the duplicated packet to those servers. This option affects the packet at Layer 4, with minor changes made to the L4 source and destination ports. This option is recommended for scenarios in which collector servers are directly connected to the ACOS device.

Parameter	Description
mirror-sa-da-repl	Mirror Source MAC Address and Destination MAC Address replacement mode replaces both the source and destination MAC addresses at Layer 2 but does not change the Layer 3 IP addressing information.
mirror-sa-repl	Mirror Source MAC Address replacement mode replaces source MAC address on incoming packets with the MAC address corresponding to virtual server on the ACOS device.

In general, most of the traffic replication options modify the headers of the duplicated packets at Layer 2 by changing the MAC address. Only one of the Traffic Replication modes alters the packets' IP address.

Default Disabled

Mode Service group

Usage Traffic replication intercepts traffic feeds, such as SNMP or Syslog packets, copies them to a buffer, and forwards duplicated packets to multiple collector servers, where data can be used to track users and devices. This is helpful for organizations needing Network Monitoring feeds replicated to multiple destinations.

When configuring the feature, after defining the VIP and setting up the real collector servers, configure a service group for the collector servers, add the real collector servers to the service group, and specify the traffic which replication mode will be used.

Unlike other replication modes, mirror mode replicates traffic to the client, in addition to replicating traffic to the server. Only lower priority servers are used, therefore it is recommended to define the collector servers as lower priority to ensure they receive the replicated traffic. For example, when SLB configuration uses the option `traffic-replication-type mirror-ip-repl`, the ACOS device should load balance traffic to the higher-priority service-group members and replicate traffic to the lower priority members or collectors.

Example The following commands configure a service group for the collector servers and add the real collector servers to the service group. Then, the commands specify that the **mirror-da-repl** traffic replication mode will be used to forward duplicated network monitoring traffic to the collector servers.

```
ACOS(config)# slb service-group SG-RS tcp
ACOS(config-slb svc group)# member RS1 0
ACOS(config-slb svc group-member:0)# priority 10
ACOS(config-slb svc group-member:0)# exit
ACOS(config-slb svc group)# member RS2 0
ACOS(config-slb svc group-member:0)# priority 5
ACOS(config-slb svc group-member:0)# exit
ACOS(config-slb svc group)# traffic-replication-type mirror-
da-repl
```

slb ssl

slb ssl-cert-revoke sampling-enable

Description Enable the AXAPI to show sampled SSL revoked certificate statistics.

Syntax

```
[no] slb ssl-cert-revoke sampling-enable counter-type
```

Parameter Value	Description
all	all
ocsp_stapling_response_good	OCSP stapling response good
ocsp_chain_status_good	Certificate chain status good
ocsp_chain_status_revoked	Certificate chain status revoked
ocsp_chain_status_unknown	Certificate chain status unknown
ocsp_request	OCSP requests
ocsp_response	OCSP responses
ocsp_connection_error	OCSP connection error
ocsp_uri_not_found	OCSP URI not found

Parameter Value	Description
ocsp_uri_https	Log OCSP URI https
ocsp_uri_unsupported	OCSP URI unsupported
ocsp_response_status_good	OCSP response status good
ocsp_response_status_revoked	OCSP response status revoked
ocsp_response_status_unknown	OCSP response status unknown
ocsp_cache_status_good	OCSP cache status good
ocsp_cache_status_revoked	OCSP cache status revoked
ocsp_cache_miss	OCSP cache miss
ocsp_cache_expired	OCSP cache expired
ocsp_other_error	Log OCSP other errors
ocsp_response_no_nonce	Log OCSP other errors
ocsp_response_nonce_error	Log OCSP other errors
crl_request	CRL requests
crl_response	CRL responses
crl_connection_error	CRL connection errors
crl_uri_not_found	CRL URI not found
crl_uri_https	CRL URI https
crl_uri_unsupported	CRL URI unsupported
crl_response_status_good	CRL response status good
crl_response_status_revoked	CRL response status revoked
crl_response_status_unknown	CRL response status unknown
crl_cache_status_good	CRL cache status good
crl_cache_status_revoked	CRL cache status revoked
crl_other_error	CRL other errors

Default Not set

Mode Configuration mode

Example

```
ACOS(config)# slb ssl-cert-revoke sampling-enable all
```

slb ssl-expire-check email-address

Description Configure email notification for certificate expiration.

Syntax

```
[no] slb ssl-expire-check email-address address [...]
[before days] [interval days]
```

Parameter	Description
address	Specifies the email addresses to which to send the notifications. You can specify up to 2 email addresses. Use a space between them.
before *days*	Specifies how many days before expiration to begin sending notification emails. You can specify 1-60. The default is 5 days.
interval *days*	Specifies how many days after expiration to continue sending notification emails. You can specify 1-5. The default is 2 days.

Default Not set

Mode Configuration mode

Usage One notification is sent per day. If a certificate is updated before expiration or at least before the configured interval, no more notification emails are sent for that certificate.

Example The following command enables certificate notifications to be sent to email address “admin1@example.com”. Expiration notifications are sent beginning 4 days before expiration and continue for 3 days after expiration.

```
ACOS(config)# slb ssl-expire-check email-address
admin1@example.com before 4 interval 3
```

slb ssl-expire-check exception

Description Exclude specific certificates from expiration notification emails.

Syntax

```
[no] slb ssl-expire-check exception
{add cert-name | delete cert-name | clean}
```

Parameter	Description
add *cert-name*	Adds a certificate to the exception list.
delete *cert-name*	Removes a certificate from the exception list.
clean	Removes all certificates from the exception list.

Default Not set

Mode Configuration mode

slb ssl-forward-proxy sampling-enable

Description Enable sampling of SSL forward-proxy events for display in the GUI or for query by the AXAPI.

Syntax

```
[no] slb ssl-forward-proxy sampling-enable
{all | cert_create | cert_expr | cert_hit | cert_miss | conn_
bypass | conn_inspect}
```

Parameter	Description
all	Enable sampling of all forward-proxy event types.
cert_ create	Enable sampling of the rate at which certificates are created.
cert_expr	Enable sampling of the rate at which created certificates are expiring.
cert_hit	Enable sampling of the rate at which certificate requests match cached certificates.
cert_miss	Enable sampling of the rate at which certificate requests di not match cached certificates.
conn_ bypass	Enable sampling the rate that SSL sessions bypassed inspection.
conn_ inspect	Enable sampling the rate that SSL sessions are inspected.

Default Sampling of SSL forward-proxy statistics is disabled.

Mode Configuration mode

slb svm-source-nat pool

Description Configure the source-NAT pool used in OCSP verification of server certificates. SVM stands for Server Verification Module.

Syntax `[no] slb svm-source-nat pool svm-pool-name`

Default None

Mode Global Configuration Mode

slb template

Description Configure an SLB template.

Syntax `[no] slb template template-type template-name`

The "no" form of this command deletes the specified slb template. If the **delete-referenced-tagged-objects** option of system config-mgmt is enabled (the default setting), the system deletes the slb template regardless of any existing references. If this option is disabled, the system checks if the slb template is being referenced by other objects and prevents deletion until all references are manually removed.

Parameter	Description
template-type	Type of template. For a list, enter the following command: **slb template ?**
template-name	Name of the template.

Default The templates have default settings, and some template types are automatically added to a virtual port depending on its service type. For information, see the ***Application Delivery Controller Guide***.

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing template. The CLI changes to the configuration level for the template.

The maximum number of templates is configurable using slb resource-usage.

Example The following command creates a TCP-proxy template named “proxy1”:

```
ACOS(config)# slb template tcp-proxy proxy1
ACOS(config-tcp proxy)#
```

slb template cache

Description Configure the ACOS device to perform transparent Web caching.

Syntax

```
[no] slb template cache template-name
```

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters the SLB Cache Template Configuration mode

Default See descriptions.

Mode Configuration mode

Usage The normal form of this command creates a RAM caching configuration template. The **no** form of this command removes the template.

You can bind only one RAM caching template to a virtual port. However, you can bind the same RAM caching template to multiple ports.

If a URI matches the pattern in more than one policy command, the policy command with the most specific match is used. For example, if a template has the following commands, content for page122 is cached whereas content for page123 is not cached:

```
policy uri /page12 cache 300
policy uri /page123 nocache
```

Wildcard characters (for example: ? and *) are not supported in RAM Caching policies. For example, if the string pattern contains “*”, it is interpreted literally, as the “*” character.

Matching is performed based on containment; all URIs containing the pattern string match the rule. For example, the following policy matches all URIs that contain the string ".jpg" and sets the cache timeout for the matching objects to 7200 seconds:

```
policy uri .jpg cache 7200
```

Example The following commands configure a RAM caching template. In this example, all the default RAM cache settings are used.

```
ACOS(config)# slb template cache ramcache
ACOS(config-ram caching)#
```

Example The following commands configure some dynamic caching policies. The policy that matches on "/list" caches content for 5 minutes. The policy that matches on "/private" does not cache content.

```
ACOS(config)# slb template cache ram-cache
ACOS(config-ram caching)# policy uri /list cache 300
ACOS(config-ram caching)# policy uri /private nocache
```

Example The following commands configure a RAM caching template that will only cache content from `www.xyz.com/news-clips`.

```
ACOS(config)# slb template cache ramcache
ACOS(config-ram caching)# default-policy-nocache
ACOS(config-ram caching)# policy uri www.xyz.com/news-clips
cache
```

accept-reload-req

Description Enables support for the following Cache-Control headers:

- Cache-Control: no-cache
- Cache-Control: max-age=0

When support for these headers is enabled, either header causes the ACOS device to reload the cached object from the origin server.

Syntax

```
[no] accept-reload-req
```

Default Disabled.

Mode SLB cache template configuration mode

Example Enable this feature:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# accept-reload-req
```

age

Description Specifies how long a cached object can remain in the ACOS RAM cache without being requested.

NOTE: This value is used if the web server specifies that the object is cacheable but does not specify for how long. If the server does specify how long the object is cacheable, then the server value is used instead.

Syntax

```
[no] age seconds
```

Parameter	Description
seconds	Number of seconds (1-999999, about 11.5 days).

Default 3600 seconds (1 hour), if the server specifies that the object is cacheable but does not specify for how long.

Mode SLB cache template configuration mode

Example Set the age to 7200 seconds (2 hours):

```
ACOS(config)#  slb template cache cache1
ACOS(config-ram caching)# age 7200
```

default-policy-nocache

Description Changes the default cache policy in the template from cache to nocache. This option gives you tighter control over content caching. When you use the default no-cache policy, the only content that is cached is cacheable content whose URI matches an explicit cache policy.

Syntax

```
[no] default-policy-nocache
```

Default Default policy is cache.

Mode SLB cache template configuration mode

Example Set the default policy to nocache:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# default-policy-nocache
```

disable-insert-age

Description Disables insertion of Age headers into cached responses.

Syntax

```
[no] disable-insert-age
```

Default Insertion of Age headers is enabled by default.

Mode SLB cache template configuration mode

Example Disable the insertion of Age headers into cached responses:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# disable-insert-age
```

disable-insert-via

Description Disables insertion of Via headers into cached responses.

Syntax

```
[no] disable-insert-via
```

Default Insertion of Via headers is enabled by default.

Mode SLB cache template configuration mode

Example Disable the insertion of Via headers into cached responses:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# disable-insert-via
```

max-cache-size

Description Specifies the maximum number of entries that can be cached per VIP.

Syntax

```
[no] max-cache-size num
```

Parameter	Description
num	Maximum number of entries that can be cached. (0-

Parameter	Description
	XXXXX). The maximum number depends on the amount of RAM and ACOS device platform.

Default The maximum configurable number per the amount of RAM and ACOS device platform.

Mode SLB template DNS configuration

Usage Specify the maximum cache entry per virtual IP.

The following table lists the maximum number of supported DNS cache entries based on the memory allocated to the platform:

Allocated RAM	Maximum DNS Cache Entries
≤ 4 GB	65,535
4 GB – 16 GB	512,000
16 GB – 128 GB	2,097,152
≥ 128 GB	4,194,304

Example The following example sets the maximum cache size to 1000:

```
ACOS(config)#  slb template cache cache1
ACOS(config-ram caching)# max-cache-size 1000
```

max-content-size

Description Specifies the maximum object size that can be cached. The ACOS device will not cache objects larger than this size. If you specify 0, no objects can be cached.

Syntax

```
[no] max-content-size num
```

Parameter	Description
num	Maximum object size in Bytes, 0-268435455 bytes (256MB).

Default 81920 bytes (80 KB).

Mode SLB cache template configuration mode

Example Set the maximum object size to 256MB:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# max-content-size 268435455
```

min-content-size

Description Specifies the minimum object size that can be cached. The ACOS device will not cache objects smaller than this size. If you specify 0, all objects smaller than or equal to the maximum content size can be cached.

Syntax

```
[no] min-content-size num
```

Parameter	Description
num	Minimum object size in Bytes, 0-268435455 bytes (256MB).

Default 512 bytes.

Mode SLB cache template configuration mode

Example Set the minimum object size to 1024 bytes:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# min-content-size 1024
```

packet-capture-template

Description Specifies Name of the packet capture template to be bind with the cache template.

Syntax

```
[no] packet-capture-template template_name
```

Default NA.

Mode SLB cache template configuration mode

Example The following example configures the packet capture template:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# packet-capture-template pcap
```

policy

Description Configure a policy for dynamic caching.

Syntax

```
[no] policy {
  local-uri pattern |
  uri pattern {cache seconds | invalidate inv-pattern |
nocache}
}
```

Parameter	Description
local-uri	Specifies the portion of a local URL string to match on (1-63 characters).
uri	Specifies the portion of the URL string to match on (1-63 characters).
cache *seconds*	Caches the content. By default, the content is cached for the number of seconds configured in the template (set by the **age** command). To override the aging period set in the template, specify the number of seconds with the **cache** command. The value can be 1-999999 seconds.
invalidate *num*	Invalidates the content that has been cached for *inv-pattern* (64 characters max). The value can be between 1-128.
nocache	Does not cache the content.

Mode SLB cache template configuration mode

Example The following commands configure some dynamic caching policies. The policy that matches on "/list" caches content for 5 minutes. The policy that matches on "/private" does not cache content.

```
ACOS(config)# slb template cache ram-cache
ACOS(config-ram caching)# policy uri /list cache 300
ACOS(config-ram caching)# policy uri /private nocache
```

remove-cookies

Description Removes cookies from server replies so the replies can be cached. RAM caching does not cache server replies that contain cookies. (Image files are an exception. RAM caching can cache images that have cookies.)

Syntax

```
[no] remove-cookies
```

Default By default, cookies are not removed.

Mode SLB cache template configuration mode

Example Enable this feature:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# remove-cookies
```

replacement-policy LFU

Description Specifies Least Frequently Used (LFU) policy is used to make room for new objects when RAM cache is full. When RAM cache is more than 90% full, ACOS device discards least-frequently used objects to ensure room for new objects.

Syntax

```
[no] replacement-policy LFU
```

Default Not enabled.

Mode SLB cache template configuration mode

Example Enable this feature:

```
ACOS(config)# slb template cache cache1
ACOS(config-ram caching)# replacement-policy LFU
```

template logging

Description Specifies a logging template to use for external logging of RAM caching events over TCP.

Syntax

```
[no] template logging name
```

Parameter	Description
name	Name of an existing logging template.

Default 512 bytes.

Mode SLB cache template configuration mode

Example Specify a logging template “extlog1” that should be used for logging RAM caching events:

```
ACOS(config)#  slb template cache cache1
ACOS(config-ram caching)# tempalte logging extlog1
```

verify-host

Description Enables the ACOS device to cache the host name in addition to the URI for cached content. Use this command if a real server that contains cacheable content hosts multiple host names (example: `www.abc.com` and `www.xyz.com`).

Syntax

```
[no] verify-host
```

Default By default, this is disabled. Host names are not cached along with URIs for cached content.

Mode SLB cache template configuration mode

Example Enable this feature:

```
ACOS(config)#  slb template cache cache1
ACOS(config-ram caching)# verify-host
```

slb template cipher

Description Configure a template of SSL cipher settings for binding to client-SSL and server-SSL templates.

Syntax

```
[no] slb template cipher template-name
```

Parameter	Description
template-name	Name of the template (1-127 characters).

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters the SLB Cipher Template configuration mode where the following commands are available.

```
[no] cipher [priority num]
```

Parameter	Description
cipher	The *cipher* can be one of the names listed in the **A10 SSL Cipher Suites List** file located on the A10 Networks Support Portal. Log in using your GLM credentials and browse to **App/Tech Notes**. You can remove (or re-add) one cipher in the template with a single command. Enter separate commands for each cipher to remove or re-add.
priority	The cipher priority value can be 1-100. The highest priority (most favored) is 100. More than one cipher can have the same priority. In this case, the strongest (most secure) cipher is used.

Default The default **priority** is 1. All ciphers within a template are enabled by default.

Mode Configuration mode

Usage

A cipher template contains a list of ciphers. A client connecting to a virtual port using the cipher template can use only ciphers that are listed in the template.

Optionally, you can assign a priority value to each cipher in the template. It is recommended that users do not leave this blank. The ACOS device uses ciphers based on priority. If the client supports the cipher that has the highest priority, that cipher is used. If the client does not support the highest-priority cipher, the ACOS device attempts to use the cipher with the second-highest priority.

Notes

- An SSL cipher template takes effect only when you apply it to a client-SSL template or server-SSL template.
- When you apply (bind) a cipher template to a client-SSL or server-SSL template, the settings in the cipher template override any cipher settings in that client-SSL or server-SSL template.
- Priority values are supported only for client-SSL templates. If a cipher template is used by a server-SSL template, the priority values in the cipher template are ignored.

Example

The following commands configure a cipher template:

```
ACOS(config)# slb template cipher cipher_tmplt1
ACOS(config-cipher)#  SSL3_RSA_DES_64_CBC_SHA priority 5
ACOS(config-cipher)#  TLS1_RSA_AES_128_SHA priority 10
ACOS(config-cipher)#  TLS1_RSA_AES_256_SHA
ACOS(config-cipher)#  end
```

This template contains three ciphers. The ACOS device attempts to use TLS1_RSA_AES_128_SHA first. If the client does not support this cipher, the ACOS device attempts to use SSL3_RSA_DES_64_CBC_SHA. If the client does not support this cipher either, the ACOS device tries to use TLS1_RSA_AES_256_SHA.

Example

The following command binds the cipher template, **cipher_tmplt1**, to the client-SSL template, **SSLInsight_ClientSide**.

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS(config-client ssl)# forward-proxy-ca-certificate
Cert123.pem key key123
```

```
ACOS(config-client ssl)# forward-proxy-enable
ACOS(config-client ssl)#  template cipher cipher_tmplt1
ACOS(config-client ssl)#  end
```

slb template connection-reuse

Description Configure re-use of established connections.

Syntax

```
[no] slb template connection-reuse template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB Connection-Reuse Template Configuration mode where the following commands are available.

Command	Description
[no] **keep-alive-conn** {preopen [number <1-1024>] | number <1-1024>}	Specifies the number of new reusable connections to open before beginning to reuse existing connections. You can specify 1-1024 connections. By default, this option is not enabled in the template, but when activated, the default value is 100. This option is applicable for both HTTP and SIP-over-TCP sessions. **Note:** Backend sessions with servers will not be reused if this parameter is set to a lower value than the limit-per-server option.
[no] **limit-per-server** *number*	Maximum number of reusable connections per server port. You can specify 0-65535. 0 means unlimited. The default is 1000 connections.

Command	Description
	Note: Backend sessions with servers will not be reused if this parameter is set to a value lower than the number of data CPUs on the ACOS device.
`[no] timeout` *seconds*	Maximum number of seconds a connection can be idle before timeing out. You can specify 60-3600 seconds; the value specified must be divisible by 60. The default is 2400 seconds (40 minutes).

Default NA

Mode Global Configuration mode

Usage You can bind only one connection-reuse template to a virtual port. However, you can bind the same connection-reuse template to multiple ports.

Example The following commands configure a connection reuse template named "conn-reuse1" and set the limit per server to 2000 re-used connections:

```
ACOS(config)# slb template connection-reuse conn-reuse1
ACOS(config-conn reuse)# limit-per-server 2000
```

Related Commands:

- show slb connection-reuse
- show cpu

slb template dblb

Description Create a template for database load-balancing (DBLB).

Syntax

```
[no] slb template dblb template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB DBLB Template Configuration mode where the following commands are available.

Command	Description
[**no**] **calc-sha1** *password*	Displays the SHA1-encrypted version of a clear text string.
[**no**] **class-list** *list-name*	Applies a class list of username-password pairs for DBLB client authentication to access the database server.
[**no**] **server-version** *type*	Specifies the *type* of database system for the DBLB server that processes database requests. For *type* you can specify one of the following: • **MSSQL2008** – MS-SQL server (version 2008 or 2008 R2) • **MSSQL2012**– MS-SQL server (version 2012) • **MySQL** – Any version of MySQL

Default The configuration does not have a default DBLB template.

Mode Configuration mode

slb template diameter

Description Configure Diameter load balancing template.

Syntax

```
[no] slb template diameter template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB Diameter Template Configuration mode where the following commands are available.

Command	Description
[**no**] **avp** *avp-num* {**int32** | **int64** | **string**} *value* [**mandatory**]	Specifies a custom AVP value to insert into Capabilities-Exchange-Request messages sent by the ACOS device to Diameter servers. For each custom AVP value to insert, you must specify the following information: • *avp-num* – Diameter AVP number. • **int32** | **int64** | **string** – Specifies the data format of the value to insert. • *value* – Specifies the value to insert. • **mandatory** – Sets the AVP mandatory flag on. By default, this flag is off (not set). You can configure up to 6 custom AVP values for insertion. Enter the command separately for each AVP value.
[**no**] **customize-cea**	Replaces the AVPs in Capabilities-Exchange-Answer (CEA) messages with the custom AVP values you configure before forwarding the messages.
[**no**] **duplicate** *avp-num pattern service-group*	Duplicates Accounting-Request messages and sends them to a separate service group. This option is useful for logging, accounting, and so on. To configure message duplication, configure real servers and the service group, and use the **duplicate** command to configure the following parameters: • *avp-num* – Diameter AVP number. • *pattern* – String pattern within the message. • *service-group* – The duplication service group, which is the service group to which to send the duplicate messages.

Command	Description
	NOTE: To place the message duplication configuration into effect, you must unbind the Diameter template from the Diameter virtual port, then rebind it. A Diameter template in which message duplication is configured can be bound to only a single virtual port.
[no] **dwr-time** *ms*	Specifies the maximum number of seconds the ACOS device will wait for the reply to a device-watch-dog message sent to a Diameter server before marking the server Down. You can specify 0-2147483647 milliseconds (ms), in 100-ms increments. The default is 10000 ms (10 seconds).
[no] **dwr-up-retry**	Specifies the number of Device Watchdog Request and Device Watchdog Answer messages required to mark a server port as up. You can specify 1-7. The default is 3.
[no] forward-to-latest-server	Disabled by default, which causes the ACOS device to forward a client Diameter message with a known session ID to a known server per info stored in the session table. When this option is enabled, the ACOS device updates the session table to the most recent server in the VIP that responds with the known session ID, and forwards client Diameter messages to that new server.
[no] forward-unknown-session-id	Disabled by default., which causes the ACOS device to drop any Diameter message from a server with an unknown session ID (with the exception of Re-Auth-Requests, which are always forwarded). When enabled, and the message is not a Re-Auth-Request, the ACOS device picks any client-side TCP

Command	Description
	connection on the same virtual port for forwarding Diameter server messages with unknown session IDs. When enabled, and the message is a Subscribe-Notifications-Request, the ACOS device picks any available client tuple for forwarding the SNR, rather than dropping it. A counter/log message will indicate that the client-tuple does not exist.
[**no**] **idle-timeout** *minutes*	Specifies the number of minutes a Diameter session remain idle before the session is deleted. You can specify 1-65535 minutes. Default is 5 minutes.
[no] load-balance-on-session-id	This option enables load balancing of diameter sessions (with different session IDs) across different servers of the service group. By default, when there is one client side TCP connections, these sessions are not load balanced across different servers. Server selection may fail when service group is configured for internal load balancing across "OCC pools".
[**no**] **message-code** *num*	Enables load balancing of Diameter message codes, in addition to those already load balanced by default. You can enable load balancing of up to 10 additional message codes: • Accounting-Request (code 271) • Accounting-Answer (code 271) • Credit-Control-Request (code 272) • Credit-Control-Answer (code 272) • Capabilities-Exchange-Request (code 257) • Capabilities-Exchange-Answer (code 257) • Device-Watchdog-Request (code 280)

Command	Description
	• Device-Watchdog-Answer (code 280) • Session-Termination-Request (code 275) • Session-Termination-Answer (code 275) • Abort-Session-Request (code 274) • Abort-Session-Answer (code 274) • Disconnect-Peer-Request/Disconnect-Peer-Answer (code 282) The ACOS device drops all other Diameter message codes by default.
[**no**] **multiple-origin-host**	Prepends the CPU ID onto the origin-host string to identify the CPU used for a given Diameter peer connection. The ACOS device establishes a separate peer connection with each Diameter server on each CPU. The multiple-origin-host option does not enable or disable this behavior. The option simply shows or hides the CPU ID in the origin-host string. This is disabled by default.
[**no**] **origin-host** *host.realm*	Sets the value of Diameter AVP 264. This AVP can be a character string and specifies the identity of the originating host for Diameter messages. Since the ACOS device acts as a proxy for Diameter, this AVP refers to the ACOS device itself, not to the actual clients. From the Diameter server's standpoint, the ACOS device is the Diameter client. Specify the origin-host in the following format: *host.realm* The *host* is a string unique to the client (ACOS device). The *realm* is the Diameter realm, specified by the origin-realm option (described below).

Command	Description
[no] **origin-realm** *string*	Sets the value of Diameter AVP 296. This AVP can be a character string and specifies the Diameter realm from which Diameter messages, including requests, are originated.
[no] **product-name** *string*	Sets the value of Diameter AVP 269. This AVP can be a character string and specifies the product; for example, “a10dra”.
[no] relaxed-ori-gin-host	Sets the relaxed origin-host format, which provides a flexible way to handle the Origin-Host AVP (Attrib-ute-Value Pair) in diameter requests.
[no] **session-age** *minutes*	Specifies the absolute limit for Diameter sessions. Any Diameter session that is still in effect when the session age is reached is removed from the ACOS session table. You can specify 1-65535 minutes. The default is 10 minutes.
[no] **terminate-on-cca-t**	Removes Diameter sessions when receiving the Server CCA-Termination message, rather than waiting for the Client Session-Terminate-Request (STR).
[no] **vendor-id** *num*	Sets the value of Diameter AVP 266. This AVP can be a numeric value and specifies the vendor; for example, “156”. Make sure to use a non-zero value. Zero is reserved by the Diameter protocol.

Default The configuration does not have a default Diameter template. If you configure one, the template has the default values described in the table above.

Mode Global Configuration Mode

Usage The Diameter load balancing template is used to enable the ACOS device to act as a proxy between Diameter clients and servers. ACOS uses SLB to select a Diameter server and forwards the client’s request to the server. ACOS then forwards the server’s reply to the client.

You can bind only one Diameter template to a virtual port. However, you can bind the same Diameter template to multiple ports.

Example The following commands configure the Diameter template:

```
ACOS(config)#slb template diameter diameter1
ACOS(config-diameter template)#origin-host 2diameter.a10com
ACOS(config-diameter template)#origin-realm a10com
ACOS(config-diameter template)#product-name a10dra
ACOS(config-diameter template)#vendor-id 156
ACOS(config-diameter template)#exit
```

See Also:

- Application Delivery Controller Guide

Related Commands:

- show slb diameter

slb template dns

Description Configure DNS template.

Syntax

```
[no] slb template dns template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

Mode Global Configuration Mode

Usage You can bind only one DNS template to a virtual port of type 'dns-udp', 'udp', or 'dns-tcp'. However, you can bind the same DNS template to multiple ports.

DNS templates are not supported with stateless load-balancing methods.

Example The following example configures the SLB DNS template `dns1`:

```
ACOS(config)#slb template dns dns1
ACOS(config-dns)#
```

Related Commands:

- show dns cache
- class-list

add-padding-to-client

Description Adds the EDNS(0) padding in DNS responses that will be sent to client. This feature is generally valid when the client is using 'TLS' for this option.

Syntax

```
[no] add-padding-to-client
```

The following options can be configured:

Command	Description
`[no] block-length`	Specify the block-length for padding the message to multiples of 468 octets. This reduces the variety of message ("fingerprint") sizes significantly.
`[no] random-block-length`	Specify the block-length for padding the message to some random numbers. This provides more variety in the resulting message sizes for a certain individual original message length.

Default This option is disabled by default.

Mode SLB Template DNS Configuration

Usage When the add padding to client option is enabled, the ACOS device adds EDNS(0) padding in DNS responses that will be sent to client.

Example The following example enables the addition of padding to DNS packets:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#add-padding-to-client random-block-length
```

See Also:

- Application Delivery Controller Guide

cache-hitcount-enable

Description Enable hit count to DNS cache entries for an individual (per) virtual port.

Syntax

```
[no] cache-hitcount-enable
```

Default The hit count to DNS cache entries per virtual port is disabled by default.

Mode SLB Template DNS Configuration

Usage When the hit count to the per virtual port DNS cache is enabled, the ACOS device records the total number of hits made to the cache.

Example The following example enables the hit count to the DNS cache entries:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#cache-hitcount-enable
```

See Also:

- Application Delivery Controller Guide

cache-record-serving-policy

Description Enable the caching record serving policy to the DNS template.

Syntax

```
[no] cache-record-serving-policy
```

The following options can be configured:

Command	Description
global	To disable the DNS template (service) level cache serving policy and follow the global level DNS cache round-robin policy. This is the default setting.
round-robin	To enable the round-robin serving of the cached DNS records for the service.
no-change	To disable the round-robin serving of the cached DNS records for the service.

Default global

Mode SLB Template DNS Configuration

Usage The cache record serving policy to the DNS template allows each service to have its own policy overwriting global policy. It is used while serving DNS cache to client queries and can adjust the order of records in response (round-robin).

Example The following command enables the dns cache round-robin policy:

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)#cache-record-serving-policy round-robin
```

cache-ttl-adjustment-enable

Description Enable for DNS entries per VIP. When this option is enabled, DNS records' TTL is adjusted according to the time elapsed since the cache was saved when ACOS responds to a DNS query with the cached DNS response.

Syntax

```
[no] cache-ttl-adjustment-enable
```

Default Disabled

Mode SLB template

Example An example is mentioned below to enable the option for DNS entries per VIP:

```
ACOS(config)# slb template dns test
ACOS(config-dns)# cache-ttl-adjustment-enable
```

category-lookup

Description Configure the DNS filtering technique using Webroot web categories.

Syntax

```
[no] category-lookup category-list-name
```

The following options can be configured:

Command	Description
drop	Deny the domains that match the web-category.
permit	Permit the domains that match the web-category and proceed with DNS resolution. If a DNS query matches more than one web-category list, an action is taken in the order of priority, with **permit** taking precedence over **drop** and **respond**.
respond	Respond with any of the following parameters when the domain matches the web-category: ○ CNAME - Send a response with a CNAME record ○ IP - Send a response with Type A record ○ IPv6 - Send a response with TYPE AAAA record. ○ NXDOMAIN - Send a response with an NXDOMAIN record. The NXDOMAIN record indicates that the domain name is not registered or does not exist. **Note**: ■ IP, IPv6, and CNAME can be configured together for one web-category list. NXDOMAIN cannot be configured along with other actions. ■ If a DNS query matches two or more web-category lists having the action **respond**, the category list with action CNAME record takes precedence.

Default Disabled

Mode SLB Template DNS Configuration

Usage Performs DNS filtering technique using Webroot web categories. You can configure web-category lists under a DNS template to match domains and take appropriate actions. You can configure up to eight web-category lists under the same DNS template. Configuring the same web-category list with different actions is prohibited.

Example The following example permits the DNS requests that match the `category1` list and proceed with DNS resolution:

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)#category-lookup category1 permit
```

See Also:

- Application Delivery Controller Guide

category-lookup-bypass

Description Specify a DNS type class-list containing a list of domains to be bypassed during web category-lookup.

Syntax

```
[no] category-lookup-bypass dns-type-list
```

Default Disabled

Mode SLB Template DNS Configuration

Usage Using the class-list, the domains that match the class-list will not be filtered out during web category-lookup and will continue with DNS resolution.

Example The following example enables the category lookup bypass for DNS records:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#category-lookup-bypass cl1
```

Example The following commands demonstrate the usage of the **category-lookup-bypass** command. As per the following configuration, any domain name that contains the term *apple* will be bypassed during web category lookup.

```
ACOS(config)# class-list my-list dns
ACOS(config-class list)#dns contains apple

ACOS(config)#slb template dns dns_temp
ACOS(config-dns)#category-lookup-bypass my-list
ACOS(config-dns)#category-lookup list2 permit
ACOS(config-dns)#category-lookup list1 drop
```

category-lookup-online-lookup

Description Enable online lookup for web category-lookup i.e., connect to the Webroot's server for domain.

Syntax

```
[no] category-lookup-online-lookup
```

Default Disabled

Mode SLB Template DNS Configuration

Usage When this option is enabled, if the domain name is not found in the local web classification database, online lookup is initiated immediately.

Example The following commands configure different web-category lists (along with the actions) for a specific DNS template. The example also demonstrates the usage of the **category-lookup-online-lookup** command.

```
ACOS(config)# slb template dns example
ACOS(config-dns)# category-lookup-online-lookup
ACOS(config-dns)# category-lookup list4 respond IP 2.2.2.2
IPv6 3:3:3::3 CNAME abc.com
ACOS(config-dns)# category-lookup list3 respond NXDOMAIN
ACOS(config-dns)# category-lookup list2 permit
ACOS(config-dns)# category-lookup list1 drop
```

class-list

Description Define granular control of DNS caching or conn-rate-limit with class-list.

Syntax

```
[no] class-list name
```

Default Disabled.

Mode SLB Template DNS Configuration

Example The following example applies the cl1 class-list to the test DNS template:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#class-list cl1
```

default-policy

Description Specifies the default action when a query does not match any class-list entries.

Syntax

```
[no] default-policy
```

The following options can be configured:

Command	Description
cache	Enable DNS caching for the query.
nocache	Disable DNS caching for the query.

Default nocache

Mode SLB Template DNS Configuration

Example The following enables DNS caching for the queries that do not match any class-list entries:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#default-policy cache
```

disable-dns-template

Description Disable the DNS template. The template remains in the configuration.

Syntax

```
[no] disable-dns-template
```

Default Disabled

Mode SLB Template DNS Configuration

Usage The command disables DNS template. It takes effect only when bound to a DNS port.

Example The following example disables the test DNS template:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#disable-dns-template
```

disable-ra-cached-resp

Description Unset DNS recursive available flag in cached response.

Syntax `[no] disable-ra-cached-resp`

Default Disabled

Mode SLB Template DNS Configuration

Example The following example unsets the recursive available flag from cached responses:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#disable-ra-cached-resp
```

disable-rpz-attach-soa

Description Disables attaching the Start of Authority (SOA) record while responding by response policy zone (RPZ).

Syntax `[no] disable-rpz-attach-soa`

Default Disabled

Mode SLB Template DNS Configuration

Example The following example disables the attaching of SOA record:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#disable-rpz-attach-soa
```

dns-cookie-cache-policy

Description Configures the virtual IP-level caching policy in the SLB template DNS for filtering DNS requests and responses having cookie records.

Syntax `[no] dns-cookie-cache-policy {served-by-cache | served-by-backend}`

Parameter	Description
served-by-cache	DNS queries with cookies are served from the DNS cache without the cookie record if a cache hit occurs.
served-by-backend	DNS queries with cookies are forwarded to the DNS backend server. Based on the backend server settings, if the server supports cookies, it responds to the

Parameter	Description
	queries with the cookie record, or if the server does not support cookies, it does not reply with cookie.

Default `served-by-cache`

Mode SLB Template DNS Configuration

Usage This command determines how DNS queries containing cookie records are handled, either by serving them from the cache (without the cookie record) or by forwarding them to the backend server (with cookie record). Configuring this policy at the SLB template level allows ACOS clients to choose between optimizing performance using the cache or getting complete responses with cookie records by forwarding queries to the DNS backend server.

Example The following sample enables the policy for handling DNS queries with cookie records by serving them from the cache.

```
ACOS(config)# slb template dns test-cookie
ACOS(config-dns)# dns-cookie-cache-policy served-by-cache
```

dns-log-enable

Description Enable logging for DNS caching.

Syntax `[no] dns-log-enable period minutes`

Default Disabled

Mode SLB Template DNS Configuration

Usage Enables logging for DNS caching. The period option specifies how often log messages are generated. You can specify 1-10000 minutes.

Example The following example enables logging for DNS caching:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#dns-log-enable period 60
```

dns64

Description Enable and configure DNS64 options for the SLB DNS template.

Note: This command and its options are not supported with DNS recursive resolution.

Syntax

```
[no] dns64 {options}
```

This command enters the DNS 64 configuration mode where the following commands are available:

Command	Description
cache	Uses a cached A-query response to provide AAAA query responses for the same hostname. For example, an A query has been cached for hostname example.com. If the client sends an AAAA query for example.com, the ACOS device does not consult the DNS server. Instead, the ACOS device uses the cached type A answer to synthesize the AAAA response, and sends the synthesized response to the client.
change-query	Changes incoming AAAA DNS query to A query. When the ACOS device receives a AAAA request from a client, this option forwards only an A request on behalf of the client. This option saves time if the DNS database contains only A records. In this case, the ACOS device does not need to wait for an error or empty response, or for the response to timeout.
parallel-query	Forwards the AAAA queries and generates the A query in parallel. **NOTE:** This option can be applied only to the dns-udp virtual port.

Command	Description
	When this option is selected, ACOS sends both an IPv6 AAAA request and an IPv4 A request at the same time on behalf of the client. When this option is enabled, the ACOS device performs DNS64 synthesis if necessary, and forwards the first valid response received to the client (empty responses and errors are invalid.)
retry	Specifies the maximum number of times the ACOS device will retry an A query if a response is not received from the DNS server. **NOTE:** This option can be applied only to the dns-udp virtual port. The configurable range is 0-15, and the default value is 3.
single-response-disable	Disables single response. In this case, the ACOS device forwards both responses to the server, if both the responses are valid. When the single-response-disable option is not configured, the first valid response is forwarded to the client.
timeout *seconds*	Specifies the maximum number of seconds the ACOS device waits for an AAAA response before sending an A query. **NOTE:** Only dns-udp port is supported for this option. The configurable range is 0-15, and the default value is 1.

Default Disabled

Mode SLB Template DNS Configuration

Usage Enables DNS64 for the DNS template to return AAAA records with synthetic IPv6 addresses for IPv4-only destinations. IPv4 service-group must be used with source-pool under the virtual port.

Example The following example enables dns64:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#dns64
ACOS(config-dns-dns64)#enable
```

Example The following commands configure the source pool under the dns-udp port for using the dns64 feature:

```
ACOS(config)#slb template dns example
ACOS(config-dns)# dns64
ACOS(config-dns-dns64)#enable
!
ACOS(config)# slb virtual-server vs 2001:20:20:20::111
ACOS(config-slb vserver)# port 53 dns-udp
ACOS(config-slb vserver-vport)# source-nat poolipv4p
ACOS(config-slb vserver-vport)# service-group mysg
ACOS(config-slb vserver-vport)# template dns example
```

dnssec-service-group

Description Specify the service group to load balance if clients' DNS query has DNSSEC OK (DO) bit set.

Syntax `[no] dnssec-service-group Service Group Name`

Default Disabled

Mode SLB Template DNS Configuration

Usage If the DNS query has DNSSEC OK (DO) bit set, the query is load-balanced to the service-group specified by this command. If the query does not have the DO bit set, it is load-balanced to the service-group bound on the virtual-port.

Example The following example specifies the service group `sg1`. A query with the DNSSEC OK (DO) bit set, will be load-balanced to the `sg1` service group.

```
ACOS(config)# slb template dns test
ACOS(config-dns)#dnssec-service-group sg1
```

See Also:

- Application Delivery Controller Guide

enable-cache-sharing

Description Allows different virtual-ports to share the DNS cache if the virtual-ports apply the same dns template.

Syntax

```
[no] enable-cache-sharing
```

Default Disabled

Mode SLB Template DNS Configuration

Example The following example enables various virtual-ports to share the DNS cache if they apply the `test` dns template:

```
ACOS(config)#slb template dns test
ACOS(config-dns)#enable-cache-sharing
```

insert-client-subnet

Description Insert Extension mechanism for DNS (EDNS (0)) Client Subnet (ECS) in the query only if it is absent.

Syntax

```
[no] insert-client-subnet ipv4 <prefix_ipv4> ipv6 <prefix_
ipv6>
```

The following parameters are provided to conceal a part of the IP address:

Command	Description
ipv4 <0-32>	Specify the source prefix length for the IPv4 address. The recommended length is 24.
ipv6 <0-128>	Specify the source prefix length for the IPv6 address. The recommended length is 56.

Default Disabled

Mode SLB Template DNS Configuration

Usage The extension contains sufficient network information and allows a recursive DNS resolver to specify the network subnet for the host on whose behalf the DNS query is made.

Example The following example inserts the extension for client sub-net and specifies the length for the source prefix for IPv4 and IPv6 addresses:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#insert-client-subnet ipv4 20 ipv6 42
```

malformed-query

Description Specify the action to take for malformed DNS queries.

Syntax

```
[no] malformed-query {drop | forward service-group-name}
```

The following actions can be configured for malformed queries:

Command	Description
drop	Drops malformed queries.
forward service-group-name	Sends the queries to the specified service group.

Default Disabled

Mode SLB Template DNS Configuration

Usage With either the drop or forward options, the malformed queries are not sent to the DNS virtual port. For the forward action, a service-group must be pre-defined.

The following packets are considered malformed when the:

- Packet length is shorter than DNS header size (12 byte).
- Packet length is longer than the **max-query-length** configuration, if present.
- DNS header QR code is non-zero.
- DNS header opcode <=5 is not considered malformed packet.

- Number of queries is zero (qdcount).
- Any of the label length is longer than 64 characters.

Example The following example indicates that malformed queries will be dropped.

```
ACOS(config)# slb template dns test
ACOS(config-dns)#malformed-query drop
```

max-cache-entry-size

Description Specify the maximum size for each cache entry, in bytes.

Syntax

```
[no] max-cache-entry-size <1-4096>
```

Default 1024

Mode SLB Template DNS Configuration

Example The following example configures the maximum size for each cache entry:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#max-cache-entry-size 2000
```

max-cache-size

Description Specifies the maximum number of entries that can be cached per VIP.

Syntax

```
[no] max-cache-size num
```

Parameter	Description
num	Maximum number of entries that can be cached. (0-XXXXX). The maximum number depends on the amount of RAM and ACOS device platform.

Default The maximum configurable number per the amount of RAM and ACOS device platform.

Mode SLB template DNS configuration

Usage Specify the maximum cache entry per virtual IP.

The following table lists the maximum number of supported DNS cache entries based on the memory allocated to the platform:

Allocated RAM	Maximum DNS Cache Entries
≤ 4 GB	65,535
4 GB – 16 GB	512,000
16 GB – 128 GB	2,097,152
≥ 128 GB	4,194,304

Example The following example sets the maximum cache size to 1000:

```
ACOS(config)#  slb template cache cache1
ACOS(config-ram caching)# max-cache-size 1000
```

max-query-length

Description Specifies the maximum length for DNS queries.

Syntax

```
[no] max-query-length num
```

Parameter	Description
num	Maximum length for a query (1-4095).

Default Unlimited

Mode SLB template DNS configuration

Example Set the maximum length of query to 900:

```
ACOS(config)#  slb template dns test
ACOS(config-dns)# max-query-length 900
```

max-udp-size

Description Configures the maximum DNS response size that ACOS is allowed to send over UDP for a specific DNS template.

Syntax

```
max-udp-size  <512-4096>
```

Default Not enabled

Mode SLB Template DNS Configuration

Usage This command sets an upper limit on the DNS response size for **dns-udp** type virtual-ports using the DNS template. If a response exceeds the configured value, ACOS sets the TC (truncated) bit in minimal response and instructs the client to retry using TCP.

NOTE: When both global and DNS template maximum UDP sizes are configured, the DNS template setting overrides the global value. If no value is configured at either level, ACOS does not apply any UDP payload size limit and forwards the DNS response to the client using the original server response directly.
The **max-udp-size** value must be smaller than the configured **edns-udp-size** value in that DNS template.

Example This example configures the maximum UDP payload size in a DNS template:

```
ACOS(config)# slb template dns dnstemplate
ACOS(config-dns)# max-udp-size 1024
```

Related Commands:

- dns-max-udp-size
- recursive-dns-resolution

negative-dns-cache enable

Description Configures negative caching of DNS responses for an individual (per) virtual port.

Prerequisite

- Enable DNS caching on template

- Enable command.

Syntax

```
[no] negative-dns-cache enable
```

This command enters the SLB DNS Template Configuration mode where the following commands are available.

Parameter	Description
bypass-query-threshold *number*	Specify the threshold for negative cache responses to be served by the ACOS device. For every threshold times the negative cache is served, the requests bypass the cache. The supported value is between 1 - 65535. The default value is 100.
cache-non-valid	Configures caching non-valid negative response. Otherwise, only valid negative responses are cached by default.
max-negative-cache-ttl *seconds*	Specify the maximum TTL period for negative responses to remain in the cache before they are removed. The supported value is between 0 - 604800 seconds. The default value is 2 hours (7200 seconds).

Default NA

Mode SLB Template DNS Configuration

Usage After configuring the feature, bind the DNS template to the virtual port (dns-tcp and dns-udp).

Example The following example configures negative caching in the SLB template and bound to virtual port:

```
ACOS(config)# slb template dns dns_negative
ACOS(config-dns)# negative-dns-cache enable
ACOS(config-dns-negative-dns-cache:)# bypass-query-threshold
20
ACOS(config-dns-negative-dns-cache:)# max-negative-cache-ttl
1024
```

```
ACOS(config-dns-negative-dns-cache:)# exit
ACOS(config-dns)# exit
ACOS(config)# slb virtual-server vip-cache 192.168.10.10
ACOS(config-slb vserver)# port 53 dns-udp
ACOS(config-slb vserver-vport)# template dns dns_negative
```

Example The following example configures both valid and non-valid negative caching in the SLB template:

```
ACOS(config)# slb template dns dns_negative
ACOS(config-dns)# negative-dns-cache enable
ACOS(config-dns-negative-dns-cache:)#cache-non-valid
ACOS(config-dns-negative-dns-cache:)# exit
ACOS(config-dns)# exit
```

Related Commands:

- dns-cache-enable

query-class-filter

Description Specify the action to be taken for the DNS query class.

Syntax

```
[no] query-class-filter {allow | deny} query-class {name | value}
```

The following actions can be configured:

Command	Description
allow	Allow only certain DNS query classes.
deny *query-class-name*	Deny only certain DNS query classes. You can specify any of the following query classes: • **INTERNET** – INTERNET query class, ID: 1 • **CHAOS** – CHAOS query class, ID: 3 • **HESIOD** – HESIOD query class, ID: 4 • **NONE** – NONE query class, ID: 254 • **ANY** – ANY query class, ID: 255 • *num* – Other query class value (1-65535)

Default All query classes are allowed

Mode SLB Template DNS Configuration

Usage When a list of query classes is specified as **allow**, the query classes which are not specified are dropped. Similarly, when a list of query classes is specified as **deny**, these query classes are dropped.

Limitation You cannot configure more than 8 query-class items. The query class IDs (mentioned above) are reserved and should not be used for Other query class (*num*).

Example The following example indicates that the queries from the INTERNET DNS query class are allowed.

```
ACOS(config)# slb template dns test
ACOS(config-dns)#query-class-filter allow
ACOS(config-dns-query-class-filter:allow)# query-class
INTERNET
```

Example The following example configures a list of DNS query classes to be denied:

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)#query-class-filter deny
ACOS(config-dns-query-class-filter:deny)#query-class ANY
ACOS(config-dns-query-class-filter:deny)#query-class INTERNET
ACOS(config-dns-query-class-filter:deny)#query-class CHAOS
ACOS(config-dns-query-class-filter:deny)#query-class 5
```

query-id-switch

Description Enables stateful query-ID-based load balancing, which distributes DNS queries on a request-ID basis.

Syntax

```
[no] query-id-switch
```

Default Disabled

Mode SLB Template DNS Configuration

Usage This command evenly distributes DNS query traffic behind a DNS proxy:

Without the query-ID-based load balancing option, multiple requests received by a DNS virtual port appear to be from the same source, if the source IP address and Layer 4 port are the same. For example, without query-ID-based load balancing, if ACOS receives multiple requests from a DNS proxy, the requests can appear to be from the same end-user, if they all have the same source IP address and Layer 4 port.

Limitation This feature applies only to DNS port 53. For other load-balanced DNS virtual ports, requests are load balanced based on the following:

- Source IP address and Layer 4 port
- Destination IP address and Layer 4 port
- Protocol (virtual port type: DNS, DNSTCP, or DNS-UDP)

This is the same as DNS load balancing without request-ID-based load balancing. The feature is "stateful" because ACOS session resources are used, and the sessions can be viewed in the session table.

Example The following example enables stateful query-ID-based load balancing.

```
ACOS(config)# slb template dns test
ACOS(config-dns)#query-id-switch
```

query-rate-monitoring

Description Enable the DNS Queries Per Second (QPS) rate monitoring.

Syntax

```
[no] query-rate-monitoring {threshold-log high num low num
[enable]}
```

The following options are available under this command:

Command	Description
threshold-log	Enables DNS QPS threshold logging. • **high** *num* – Specifies the high (1-64000000) threshold value for DNS QPS logging. ◦ **low** *num* – Specifies the low (1-63999999) threshold value for DNS QPS logging.

Command	Description
	■ **enable** – Enables the system to generate event logs when the QPS value crosses the configured thresholds.

Default Disabled

Mode SLB Template DNS Configuration

Example The following example enables QPS rate monitoring.

```
ACOS(config)# slb template dns test
ACOS(config-dns)#query-rate-monitoring threshold-log high 6000
low 5000 enable
```

query-type-filter

Description Specify the action to be taken for the DNS query type. You can specify upto 16 query types.

Syntax

```
[no] query-type-filter {allow | deny} query-type {type-name |
value}
```

The following actions can be taken for DNS query types:

Command	Description
allow	Allow only certain DNS query types. The query types which are not specified are dropped.
deny	Deny only certain DNS query types. The query types are dropped. You can specify any of the following query types: • **A** – Address record, query type ID: 1 • **AAAA** – IPv6 Address record, query type ID: 28 • **CNAME** – Canonical name record, query type ID: 5

Command	Description
	• **MX** – Mail exchange record, query type ID: 15 • **NS** – Name server record, query type ID: 2 • **SRV** – Service locator, query type ID: 33 • **PTR** – PTR resource record, query type ID: 12 • **SOA** – Start of authority record, query type ID: 6 • **TXT** – Text record, query type ID: 16 • **ANY** – All cached record, query type ID: 255 • *num* – Other record type value (1-65535). The query type IDs (mentioned above) are reserved and should not be used for this record type.

Default All query types are allowed

Mode SLB Template DNS Configuration

Example The following example configures a list of DNS query-types to be allowed:

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)# query-type-filter allow
ACOS(config-dns-query-type-filter:allow)# query-type ANY
ACOS(config-dns-query-type-filter:allow)# query-type PTR
ACOS(config-dns-query-type-filter:allow)# query-type 7
ACOS(config-dns-query-type-filter:allow)# query-type 8
```

recursive-dns-resolution

Description Enable recursive DNS resolver feature and configure the required options.

Syntax

```
[no] recursive_dns_resolution
```

This command enters the SLB DNS Template recursive DNS resolution mode where the following command options are available.

Command	Description
csubnet-retry	Specify this option to retry if the server responds with REFUSED rcode for queries with EDNS(0) client subnet inserted. This option works only if **insert-client-subnet** is configured. In case the server responds with REFUSED rcode for queries with EDNS(0) client subnet inserted, the original query that is specified without inserted subnet is retried.
default-recursive	Enable default recursive mode to forward query to the bound service-group if the hostnames match. Otherwise, initiate recursive resolution to resolve clients' DNS query.
dnssec-validation *{enabled | disabled}*	Enable or disable DNSSEC validation on responses received before the resolver continues to resolve a CNAME or sends the response to clients.
edns-udp-size *<512-4096>*	Specify the UDP payload size field of EDNS (0) OPT record used by ACOS when generating recursive resolver (RR) queries. The default value is 4096. This value indicates the maximum UDP payload size that ACOS can receive, and Internet DNS servers should comply with this limit.

Command	Description
	NOTE: The configured **edns-udp-size** value must be greater than or equal to the max-udp-size value configured under that DNS template. If no **max-udp-size** value is configured under the DNS template, then **edns-udp-size** value must be greater than or equal to the dns-max-udp-size value configured globally.
force-cname-resolution *{enabled | disabled}*	Enable or disable CNAME resolution option when the matching answer record also exists in the CNAME response packet.
full-response	Serve all the records (authority and additional) when applicable. Otherwise, minimal response (only answer section records) is served.
gateway-health-check	Optional. Enable health check to recursive gateway based on current system configuration. The following options are available under this command: • *interval* - Specify the interval (in seconds) between the health check attempts. The range can be 1-300 seconds. The default value is 10 seconds. The health check attempt begins only when the ongoing health check is complete. • *ns-cache-lookup* - Enables or disables NS record cache lookup during the

Command	Description
	health check process. • *query-name* - Specify the query name used in the probe queries. The default value is a10networks.com. The query length can be 1-255 characters. • *query-type* - Specify the query (DNS record) type used in the probe queries. The query type can be A, AAAA, CNAME, MX, NS, SRV, PTR, SOA, TXT, or other record type value between 1-65535. The default is an A record. • *retry* - Specify the maximum number of DNS query retries to send at each server level before determining that the health check failed. The range can be 1-6. The default value is 6. • *retry-multi* - Specify the number of times the health check consecaflowutively fails before determining that the gateway is DOWN. The range can be 1-10. The default value is 1. • *timeout* - Specify the period (in seconds) that ACOS waits for a reply to a health check. The range can be 1-6 seconds. The default value is 5 seconds. • *up-retry* - Specify the number of times the health check consecutively passes before determining the gateway is UP. The range can be 1-10. The default value is 1.

Command	Description
	NOTE: The following **recursive DNS resolution** level configurations will be applied on health check traffic. • **ipv4-nat-pool** and **ipv6-nat-pool** • **lookup-order** • **max-trials** • **ns-cache-lookup** (to generate NS and A/AAAA type cache from recursive resolution)
hostnames	Optional. Bind the DNS type class-list name to perform top-level domain (TLD) resolution for a subset of domain names instead of all the DNS queries.
ipv4-nat-pool *NAME*	Mandatory. Bind an IPv4 source NAT pool or pool group to query the TLD servers.
ipv6-nat-pool *NAME*	Mandatory. Bind a IPv6 source NAT pool or pool group to query the TLD servers. You can configure: • Either an IPv4 or an IPv6 NAT pool • An IPv6 NAT pool while the virtual server is IPv4 or vice-versa • Both types of NAT pools at the same time.
lookup-order query-type *order-option*	Optional. Specify the lookup order for each DNS query type individually using the preferred IP protocol for resolver to perform lookup through IPv4 or IPv6.

Command	Description
	The following order options are available: • **A** - Address record • **AAAA** - IPv6 Address record • **CNAME** - Canonical name record • **MX** - Mail exchange record • **NS** - Name server record • **SRV** - Service locator • **PTR** - PTR resource record • **SOA** - Start of authority record • **TXT** - Text record • **ANY** - All cached record • **<1-65535>** - Other query type value. You can lookup: ◦ **ipv4-precede-ipv6** - Recursive lookup is performed via IPv4. In case of failure, IPv6 is used. ◦ **ipv6-precede-ipv4** - Recursive lookup is performed via IPv6. In case of failure, IPv4 is used.
max-trials	Optional. This command configures the maximum number of total trials that ACOS performs, cumulative of all levels based on per client DNS query, before quitting the recursive process. The configurable range is 1-255. The default value is 255.
ns-cache-lookup {enabled | disabled}	Enable or disable NS cache lookup.

Command	Description
ns-longest-match {enabled | disabled}	Look up the longest-matched NS when **ns-cache-lookup** is enabled.
parallel-queries	Optional. Specify the number of parallel DNS queries that can be sent to multiple resolvers for DNS recursive resolution. The default value is 1 and the configurable range is 1-15.
request-for-pending-resolution	Specify the action to take during an ongoing pending resolution. The following actions can be defined: • drop - Drop the request during an ongoing pending resolution. • respond-with-servfail - Respond with SERVFAIL for the request during an ongoing pending resolution. This is the default option. • start-new-resolution - Start a new resolution of the request.
retries-per-level	Optional. This command configures the maximum number of retries at each server level of the DNS resolution process before closing client connection. The configurable range is 1-6. The default value is 6.
udp-retry-interval	Optional. This command configures the interval for UDP DNS retries. The configurable range is 1-6 seconds. The default value is 1.
use-service-group-response{enabled | disabled}	Enable or disable backend service group response and skip recursive resolution.

Default DNS template recursive DNS resolution command options have the default settings described in the table above.

Mode SLB Template DNS Configuration

Usage The recursive DNS resolver:

- Supports **dns-udp** and **dns-tcp** type virtual server ports only.
- Supports caching the responses only when DNS caching is configured globally using **dns-cache-enable** command under 'slb common' module.
- Does not support the **query-id-switch** command when enabled on any DNS template in the same L3v partition.

Example The following example enables DNSSEC validation on responses received before the resolver continues to resolve a CNAME or sends the response to clients:

```
ACOS(config)#slb template dns dns1
ACOS(config-dns)#recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)#dnssec-validation
enabled
```

Example The following commands configure the health monitoring for recursive gateway:

```
ACOS(config)# slb template dns temp
ACOS(config-dns)# recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)#gateway-health-check
ACOS(config-dns-recursive-dns-resolution-...)# interval 4
ACOS(config-dns-recursive-dns-resolution-...)# up-retry 2
```

Example The following commands demonstrate the usage of **insert-client-subnet** and **csubnet-retry**:

```
ACOS(config)# slb template dns temp
ACOS(config-dns)# insert-client-subnet ipv4 24 ipv6 56
ACOS(config-dns)# recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)# csubnet-retry
```

Example The following example shows how to configure the EDNS(0) UDP payload size for recursive DNS queries:

```
ACOS(config)# slb template dns dnstemplate
ACOS(config-dns)# recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)# edns-udp-size 1024
```

Related Commands:

- dns-max-udp-size
- max-udp-size

redirect-to-tcp-port

Description Enables authentication for DNS requests received over UDP.

Syntax

```
[no] redirect-to-tcp-port
```

Default Disabled

Mode SLB template DNS configuration

Usage When this feature is enabled, ACOS drops the UDP DNS request from a client, and sends the client a DNS Truncate message. To pass DNS authentication, the client must resend the DNS request over TCP.

Example The following example redirects the DNS requests received over UDP to TCP:

```
ACOS(config)# slb template dns test
ACOS(config-dns)# #redirect-to-tcp-port
```

remove-aa-flag

Description Make answers created from cache non-authoritative.

Syntax

```
[no] remove-aa-flag
```

Default Disabled

Mode SLB template DNS configuration

Example The following configuration makes the answers created from the cache non-authoritative:

```
ACOS(config)# slb template dns test
ACOS(config-dns)# remove-aa-flag
```

remove-edns-csubnet-to-server

Description Remove EDNS (0) client subnet from the client queries before forwarding to the server.

Syntax

```
[no] remove-edns-csubnet-to-server
```

Default Disabled

Mode SLB template DNS configuration

Example The following configuration removes EDNS (0) client subnet from the client queries:

```
ACOS(config)# slb template dns test
ACOS(config-dns)# remove-edns-csubnet-to-server
```

remove-padding-to-server

Description Removes the EDNS(0) padding from client queries before forwarding to the server. This feature is generally valid when the client is using TLS.

Syntax

```
[no] remove-padding-to-server
```

Default Disabled

Mode SLB template DNS configuration

Example The following configuration removes the EDNS(0) padding from client queries before forwarding to the server:

```
ACOS(config)#  slb template dns test
ACOS(config-dns)# remove-padding-to-server
```

response-rate-limiting

Description Configure the options for DNS Response Rate Limiting.

Syntax

```
[no] response-rate-limiting
```

Specify one of the following options under **response-rate-limiting**:

Command	Description

Command	Description
`TC-rate` *num*	Specify the rate at which the DNS server responds with truncated (TC) bit or response. Every nth rate limited request will get a TC bit response forcing the requestor to use TCP. The value can be set from 2 - 10. For example, if the TC rate is set to 3, then one out of every 3 rate-limited (dropped) queries will receive a truncated response. **NOTE:** `TC-rate` and `slip-rate` are mutually exclusive commands.
`action` *option*	Specify the action to be taken if DNS response rate limit exceeds. The following options can be configured: • **`log-only`** - Only log rate-limiting, but does not actually apply rate limits. Selecting this option will enable “log only” behavior for rate-limiting. ACOS will behave as if the queries are being rate-limited. Logs will be sent out and counters for Dropped, Allowed, and Slipped are incremented, even though these packets were actually permitted to pass. Enabling this option also requires selecting the “enable-log” configuration. • **`rate-limit`** - Rate-Limit based on configuration (Default). • **`whitelist`** - This effectively disables DNS rate-limiting.

Command	Description
`enable-log`	Enables “log only” behavior. It enables logs for rate-limiting entries. Actual actions on traffic will depend on what the user configures for the action. This option is disabled by default, due to possible high log volume. If enabled, this generates logs which are themselves rate-limited at a rate of one per minute. The content of logs indicates if rate-limiting is occurring for a particular source and FQDN combination.
`filter-response-rate` *`max queries per second`*	Specify the maximum allowed request rate for the filter table. The default value is set to 10 queries per second. The value can be from 1 - 1000 queries per second. This value should match the rate of DNS queries during normal traffic patterns. This is the first “filter table” for normal DNS requests. Once a client (source + FQDN) exceeds this rate, then subsequent requests are moved to the “rate-limit entry table” to monitor for potential threats. **NOTE:** Any changes to the maximum table entries requires disabling and then re-enabling the template on the virtual port to which it is bound.
`match-subnet {`*`/masklength`* `|` *`ipv4-address`*`}`	Specify the IPv4 subnet mask length to match. Rate-limiting is performed per requestor's IP address where the IP

Command	Description
	address is grouped to create an IPv4 address block. You can specify one of the following filters to match. • */masklength* - Specify the IP subnet mask. For example, you can specify */24*. • *filter-mask* - Specify the IPv4 address. For example, you can specify *0.0.0.255* on a 24-bit subnet. Where 0 represents match, and 255 represents ignore.
`match-subnet-v6` *num*	Specify the IPv6 subnet mask length to match. Rate-limiting is performed per requestor's IP address where the IP address is grouped to create an IPv6 address block. The value can be between 1 to 128.
`response-rate`	This is the maximum allowed request rate for the filter. Configure a value from 1 - 1000 queries per configured `window`. Responses exceeding this rate will be dropped. This parameter maps to the second of the two tables, the “rate-limit entry table”, and is used for abusive DNS requests. Once a client exceeds the rate in the filter table, then subsequent requests from that (source + FQDN) are moved to this “rate-limit entry table” to monitor them more closely for potential threats.
`rrl-class-list list-name`	Specify the class list for DNS response rate limiting, with length 1-63.

Command	Description
`slip-rate`	Enables some portion of traffic to pass through to the target (whose IP address is being spoofed) even during an attack. If a value is configured for the slip rate, then every n'th response that would have been rate-limited will instead be let through. The slip rate must be set from 2 - 10, and should approximate the retry count for regular queries. Setting the **`slip-rate`** to zero effectively disables this option.
`src-ip-only`	Enable response rate limiting based on source IP only instead of FQDN.
`window`	Configures the rate-limiting-window, which is the time interval over which rates are measured and during which memory of rate-limit excesses is retained. If a client asks for the same DNS mapping too many times, then similar queries from that same client will be dropped for the rest of the window. Default is 1 second. Range is 1 - 60 seconds. This option impacts `response-rate` and `slip-rate`.

Default Disabled

Mode SLB template DNS configuration

Usage This command and its options enable ACOS to support DNS Response Rate Limiting (RRL). This feature is used to mitigate risks caused by DNS amplification or reflection attacks. DNS RRL enables ACOS to effectively control the rate of DNS server responses associated with the DNS requests flagged as potentially malicious.

Example The following example configures the rate-limiting window to 2 seconds:

```
ACOS(config)# slb template dns test
ACOS(config-dns)#response-rate-limiting
```

```
ACOS(config-dns-response-rate-limiting)# window 2
```

See Also:

- DDoS Mitigation Guide

rpz

Description Specifies the Response Policy Zone (RPZ) file to be bound with the DNS template.

Syntax

```
[no] rpz seq_id file_name logging {enable action}
```

The following parameters can be configured:

Command	Description
seq_id	Specify the sequential ID (1-8). • *file_name*: Specify the name of the RPZ file, 1-63 characters. ◦ **logging enable**: Use this command to log the RPZ triggered actions. The following actions take effort. ◦ *action*: When the logging is enabled, you can specify any of the following actions: ■ **drop**: Log the drop action ■ **pass-thru**: Log the pass-thru action ■ **nxdomain**: Log the nxdomain action ■ **nodata**: Log the nodata action ■ **tcp-only**: Log the tcp-only action ■ **local-data**: Log the local-data action

Default Disabled

Mode SLB template DNS configuration

Example The following command binds the RPZ to the *temp1_dns* template:

```
ACOS(config)# slb template dns temp1_dns
ACOS(config-dns)# rpz 1 A10.rpz
ACOS(config-dns-rpz)# logging enable
ACOS(config-dns-rpz-logging:enable)# rpz-action drop
ACOS(config-dns-rpz-logging:enable)# rpz-action tcp-only
```

template

Description Specifies the DNS logging template.

Syntax `[no] template dns-logging template_name <1-127>`

Default Disabled

Mode SLB template DNS configuration

Example The following example binds the **temp1** DNS logging template to the **test** dns template:

```
ACOS(config)#  slb template dns test
ACOS(config-dns)# template dns-logging temp1
```

tld-filter-log-enable

Description Enable DNS TLD filter logging when the packets are dropped by tld-filter.

Syntax `[no] tld-filter-log-enable`

Default Disabled

Mode SLB template DNS configuration

Example Enable the logging of DNS TLD filter:

```
ACOS(config)#slb template dns test
ACOS(config-dns)#tld-filter-log-enable
```

tld-filter-white-list

Description Specifies the name of the class-list to be used for TLD filter whitelist.

Syntax `[no] tld-filter-white-list class-list-name`

Default Disabled

Mode SLB template DNS configuration

Usage Specify the name of the class-list (string-case-insensitive) to be used for TLD filter whitelist. The class-list contains the whitelisted top-level domains (TLDs).

Example The following example configures the `cl1` class-list (string-case-insensitive) for TLD filtering:

```
ACOS(config)# slb template dns test
ACOS(config-dns)# tld-filter-white-list policy_cl1
```

udp-retransmit

Description Specifies the policy to retransmit UDP packets.

Syntax

```
[no] udp-retransmit {max-trials <1-5> | retry-interval <1-400>}
```

The following options can be configured:

Command	Description
max-trials	Specify the total number of times to try DNS query to the server before closing client connection. The default value is 3.
retry-interval	Specify the DNS Retry Interval value. The value can be 1 - 400 in units of 100ms. The default value is 10 (1000ms/1sec).

Mode SLB template DNS configuration

Example The following example configures the maximum number of retrials for retransmitting UDP packets and the retry interval:

```
ACOS(config)#slb template dns test
ACOS(config-dns-udp-retrnsmit)#max-trials 4
ACOS(config-dns-udp-retrnsmit)#retry-interval 40
```

slb template dns-logging

Description Configure DNS request and response query logging.

NOTE: Only remote log is supported for DNS logging.

Syntax

```
slb template dns-logging template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

Default Disabled

This command enters the SLB DNS Logging Template Configuration mode where the following commands are available:

Command	Description
custom-log [request | response | timeout]	Customize the logging template for DNS queries (request, response, or timeout events). The following options are available: • **request** – Log the DNS request received from the client. ◦ **enable** – Enable custom logging for requests. The default value of enable is not set. ◦ **format** – Specify the request log message format. The default value of format is empty. ◦ **log-filter RPZ** – Sets log filter for RPZ request type only. • **response** – Log the DNS response sent to the client. ◦ **enable** – Enable custom logging for responses. The default value of enable is not set. ◦ **format** – Specify the response log message format. The default value of format is empty.

Command	Description

	• **timeout** – Log when a DNS request connection times out.
	  ◦ **enable** – Enable custom logging for timeout events. The default value of enable is not set.
	  ◦ **format** – Specify the log message format. The default value of format is empty.

disable	Disable the DNS Logging template.
protocol	Log the DNS protocol. The following options are available: • **both** – Log DNS over TCP and UDP. • **tcp** – Log DNS over TCP. • **udp** – Log DNS over UDP.
request-section	Log the DNS request section. The following options are available: • **all** – Log the DNS header and question sections. • **header** – Log only the DNS header section. • **question** – Log only the DNS question section.
response-include-rcode	Log the RCODE (response code) field in DNS response log. If you configure the **response-section** option, then the DNS header information is also included.
response-section	Log the content from DNS server response. The following options are available: • **all** – Log DNS header information, answer, authority and additional sections. • **header** – Log only the DNS header information. • **answer** – Log only the DNS header information and answer section.

Command	Description
response-tuple	Log tuple information from DNS client or server response. The following options are available: • **client-side** – Log the tuple information from the client-side response. • **server-side** – Log the tuple information from the server-side response.
response-type config	Log the RDATA record type in DNS response logs. The following option is available: • **type** <record-type> - Specifies the response record type. After selecting a record type, you can configure its additional parameters such as length-limit. The length-limit can be set per record type in the range 0–256 bytes. For the all option, the maximum allowed length-limit is 1024 bytes. Supported record-types are TXT, RRSIG, TSIG, DNSKEY, DS, CAA, NAPTR, OPT.
standard-log	Define a standard logging template for DNS queries (request). The following options are available: • **request** – Log the DNS request received from client. ◦ **log-filter RPZ** – Sets log filter for RPZ request type only.
type	Log the DNS type. • **query** – DNS query logging. • **response** – DNS response logging. • **both** – DNS query and response logging.

Mode Configure

Usage

ACOS provides two types of DNS logging methods to support different operational needs, one for simplified standard logging and another for detailed custom logging. For more information on both the logging methods, see *DNS Logging* chapter in the *Application Delivery Controller Guide.*

You must remove all CGNv6 configurations before making SLB configurations (including aFlex, AAM, GSLB, and Overlay).

Example

The following example creates the **dnslog** DNS logging template:

```
ACOS(config)#slb template dns-logging dnslog
ACOS(config-dns-logging)# request-section all
ACOS(config)# slb virtual-server vip 192.168.10.10
ACOS(config-slb vserver)# port 53 dns-udp
ACOS(config-slb vserver)# template dns dnslog
```

The following commands bind the DNS logging template to slb template dns:

```
ACOS(config)#slb template dns dns_test
vThunder(config-dns)#template dns-logging dnslog
```

The DNS log created by the command uses the following conventions:

- **proto** – The protocol being used: UDP, TCP, or both
- **src** – Source IP of the incoming packet
- **spt** – Source port of the incoming packing
- **dest** – Destination IP address
- **dpt** – Destination port of the packet
- **type** – Query is the only supported type
- **queryId** – Query ID of the request

The header log includes the following:

- Opcode: Query, IQuery, Status, Reserved, Update, and Notify
- Header Flags:
  - AA (Authoritative Answer) — This bit is set to 1 when the responding server is authoritative for the domain name's zone specified in the Question section. This bit is set to 0 when the response is *not* authoritative.

- CD (Checking Disabled) — This bit requests that the responding server disable signature validation and not check DNSSEC records.
- RA (Recursion Available) — This bit is set to 1 or 0 when the responding server supports recursive queries. This can optionally be used by the querying device in the future.
- RD (Recursion Desired) — When included in a query, it serves as a request for the receiving server to respond to the query recursively if possible. The value of this bit is the same in the query and the response.
- TC (Truncation) — This bit is set to 1 to indicate that the response was truncated because it exceeds the maximum length permitted by the transport mechanism. Because TCP has no limit for messages, and UDP limits messages 512 bytes, this bit also indicates that the message was sent using UDP. It is often possible for the client to establish a TCP session to avoid truncation.
- Z (Zero) — The three reserved bits are set to 0 (zero).

The following example shows the DNS Request Header (CEF and Syslog) that results from specifying the **request-section header**:

```
Apr 02 2019 20:48:55 Info        [ACOS]: vThunder
CEF:0|A10|ADC|4.1.4-adc-420-feat-238627|486715039831556097|Log
DNS Request Header|2|proto=UDP src=10.1.1.1 spt=39093
dst=30.1.10.1 dpt=53 cs1=Query cs1Label=Query cn1=33511
cn1Label=Query ID cs2=Query cs2Label=Opcode cs3=RD|AD
cs3Label=Header Flag cn2=1 cn2Label=Question Count cn3=0
cn3Label=Answer Record Count cn4=0 cn4Label=Authority Record
Count cn5=1 cn5Label=Additional Record Count
Apr 02 2019 20:51:43 Info        [ACOS]: vThunder
CEF:0|A10|ADC|4.1.4-adc-420-feat-238627|486715039831556097|Log
DNS Request Header|2|proto=TCP src=10.1.1.1 spt=42928
dst=30.1.10.1 dpt=53 cs1=Query cs1Label=Query cn1=29521
cn1Label=Query ID cs2=Query cs2Label=Opcode cs3=RD|AD
cs3Label=Header Flag cn2=1 cn2Label=Question Count cn3=0
cn3Label=Answer Record Count cn4=0 cn4Label=Authority Record
Count cn5=1 cn5Label=Additional Record Count
```

```
Apr 02 2019 20:47:29 Info        [ACOS]:UDP 10.1.1.1.50850
30.1.10.1.53 Type=Query QueryId=28245 Opcode=Query
HeaderFlag=RD|AD QDCount=1 ANCount=0 NSCount=0 ARCount=1
Apr 02 2019 20:50:28 Info        [ACOS]:TCP 10.1.1.1.52597
30.1.10.1.53 Type=Query QueryId=33027 Opcode=Query
HeaderFlag=RD|AD QDCount=1 ANCount=0 NSCount=0 ARCount=1
```

The following example shows the DNS Request Question (CEF and Syslog) that results from specifying the **request-section question**:

```
Apr 02 2019 20:49:10 Info        [ACOS]: vThunder
CEF:0|A10|ADC|4.1.4-adc-420-feat-238627|486715039831556098|Log
DNS Request Question|2|proto=UDP src=10.1.1.1 spt=42839
dst=30.1.10.1 dpt=53 cs1=Query cs1Label=Query cn1=32748
cn1Label=Query ID dhost=server.pradeep.com cs2=A
cs2Label=Query Type cs3=IN cs3Label=Query Class
Apr 02 2019 20:51:59 Info        [ACOS]: vThunder
CEF:0|A10|ADC|4.1.4-adc-420-feat-238627|486715039831556098|Log
DNS Request Question|2|proto=TCP src=10.1.1.1 spt=38573
dst=30.1.10.1 dpt=53 cs1=Query cs1Label=Query cn1=50512
cn1Label=Query ID dhost=server.pradeep.com cs2=A
cs2Label=Query Type cs3=IN cs3Label=Query Class
Apr 02 2019 20:47:43 Info        [ACOS]:UDP 10.1.1.1.54170
30.1.10.1.53 Type=Query QueryId=7280 dhost=server.pradeep.com
QueryType=A QueryClass=IN
Apr 02 2019 20:50:42 Info        [ACOS]:TCP 10.1.1.1.33086
30.1.10.1.53 Type=Query QueryId=37115 dhost=server.pradeep.com
QueryType=A QueryClass=IN
```

The following example shows the DNS Request Header and Questions (CEF and Syslog) that results from specifying the **request-section all**:

```
Apr 02 2019 20:49:25 Info        [ACOS]: vThunder
CEF:0|A10|ADC|4.1.4-adc-420-feat-238627|486715039831556099|Log
DNS Request Header and Questions|2|proto=UDP src=10.1.1.1
spt=35419 dst=30.1.10.1 dpt=53 cs1=Query cs1Label=Query
cn1=6966 cn1Label=Query ID cs2=Query cs2Label=Opcode cs3=RD|AD
cs3Label=Header Flag cn2=1 cn2Label=Question Count cn3=0
cn3Label=Answer Record Count cn4=0 cn4Label=Authority Record
Count cn5=1 cn5Label=Additional Record Count
dhost=server.pradeep.com cs4=A cs4Label=Query Type cs5=IN
cs5Label=Query Class
Apr 02 2019 20:52:14 Info        [ACOS]: vThunder
CEF:0|A10|ADC|4.1.4-adc-420-feat-238627|486715039831556099|Log
DNS Request Header and Questions|2|proto=TCP src=10.1.1.1
spt=56362 dst=30.1.10.1 dpt=53 cs1=Query cs1Label=Query
cn1=44728 cn1Label=Query ID cs2=Query cs2Label=Opcode
cs3=RD|AD cs3Label=Header Flag cn2=1 cn2Label=Question Count
cn3=0 cn3Label=Answer Record Count cn4=0 cn4Label=Authority
Record Count cn5=1 cn5Label=Additional Record Count
dhost=server.pradeep.com cs4=A cs4Label=Query Type cs5=IN
cs5Label=Query Class
Apr 02 2019 20:47:57 Info        [ACOS]:UDP 10.1.1.1.33912
30.1.10.1.53 Type=Query QueryId=62463 Opcode=Query
HeaderFlag=RD|AD QDCount=1 ANCount=0 NSCount=0 ARCount=1
dhost=server.pradeep.com QueryType=A QueryClass=IN
Apr 02 2019 20:51:28 Info        [ACOS]:TCP 10.1.1.1.45824
30.1.10.1.53 Type=Query QueryId=27573 Opcode=Query
HeaderFlag=RD|AD QDCount=1 ANCount=0 NSCount=0 ARCount=1
dhost=server.pradeep.com QueryType=A QueryClass=IN
```

Example The following example logs the DNS response and include **RCODE** field in the log output:

```
ACOS(config)# slb template dns-logging dns180
ACOS(config-dns-logging)# response-include-rcode
ACOS(config-dns-logging)# response-section all
```

After enabling the **response-include-rcode** and **response-section all** options, the following DNS response logs (in CEF and Syslog formats) are generated:

CEF Log Example

```
proto=UDP src=32.100.100.100 spt=60 dst=10.211.10.2 dpt=52050
cs1=Response cs1Label=Response cs2=backend cs2Label=Response
Source cn1=1207 cn1Label=Query ID cs3=Query cs3Label=Opcode
cs4=RD|RA cs4Label=Header Flag cs5=03 cs5Label=RCODE cn2=1
cn2Label=Question Count cn3=0 cn3Label=Answer Record Count
cn4=1 cn4Label=Authority Record Count cn5=0
cn5Label=Additional Record Count cs6=Authority section SOA IN
10800 a.root-servers.net nstld.verisign-grs.com 2024072400
1800 900 604800 86400;] cs6Label=response content
```

Syslog Example

```
UDP 32.100.100.100 60 10.211.10.2 36545 Type=Response
source=backend QueryId=13984 Opcode=Query HeaderFlag=AA|RD|RA
RCODE=00 QDCount=1 ANCount=3 NSCount=2 ARCount=4
response=Answer section [www.example.com CNAME IN 86400
services.example.com;services.example.com A IN 86400
10.212.2.21;services.example.com A IN 86400 10.212.2.20;]
Authority section [example.com NS IN 86400
dns1.example.com;example.com NS IN 86400 dns2.example.com;]
Addition section [dns1.example.com A IN 86400
10.212.2.20;dns1.example.com AAAA IN 86400
aaaa:bbbb::1;dns2.example.com A IN 86400
10.212.2.22;dns2.example.com AAAA IN 86400 aaaa:bbbb::2;]
```

Example The following example configures the **custom-log** in the DNS logging template:

```
ACOS(config)#slb template dns-logging dns180
ACOS(config-dns-logging)# custom-log request
ACOS(config-dns-logging-custom-log:request)# format "queryid
is $queryId$ opc is $opcode$ rcode is $rcode$ rcode string is
$rcodestr$"
ACOS(config-dns-logging-custom-log:request)# enable
ACOS(config-dns-logging-custom-log:request)# exit
ACOS(config-dns-logging)# custom-log response
ACOS(config-dns-logging-custom-log:response)# format "querid
is $queryId$ opc is $opcode$ Response src is $respsrc$ Rcode
is $rcode$ NAT info is $snatinfo$"
```

```
ACOS(config-dns-logging-custom-log:response)# enable
ACOS(config-dns-logging-custom-log:response)# exit
```

Example The following example configures the **custom-log** in the DNS logging template to log DNS query timeout with a custom message format:

```
ACOS(config)# slb template dns-logging log_template_name
ACOS(config-dns-logging)# custom-log timeout
ACOS(config-dns-logging-custom-log:timeout)# format "Djtimeout
$src$#$spt$ $dst$#$dpt$ $snatinfo$ $proto$ $queryid$
$recordcounters$ $opcode$ $headerflag$ $queryinfo$ $qdcount$
$ancount$ $nscount$ $arcount$"
ACOS(config-dns-logging-custom-log:timeout)# enable
```

Example The following example configures a DNS logging template named **aaaa** that applies RPZ-based filtering for both standard and custom DNS request logs:

```
ACOS(config)#slb template dns-logging aaaa
ACOS(config-dns-logging)# standard-log request
ACOS(config-dns-logging-standard-log:request)# log-filter RPZ
ACOS(config-dns-logging-standard-log:request)# exit
ACOS(config-dns-logging)# custom-log request
ACOS(config-dns-logging-custom-log:request)# log-filter RPZ
ACOS(config-dns-logging-custom-log:request)# exit
```

slb template doh

Description Configure DNS over HTTP/HTTPs (DoH) template for SLB.

Syntax

```
[no] slb template doh doh_template-name
```

Replace *doh_template-name* with the name of the template, 1-127 characters.

This command enters the SLB DNS over HTTP Template Configuration mode where the following commands are available.

Command	Description
`conn-reuse {enable | disable}`	Specify action to enable or disable connection reuse. Connections are established to each server when a server is first selected for a client request and is not disconnected immediately. The connections can be re-used for future client requests. When a connection is used for a DNS request and is awaiting a response, it is not eligible for a second request. If a new client request is received, then a different available connection, or a new connection to the server will be used. **`conn-reuse`** applies to both TCP as well as UDP connections. However, the behaviour slightly differs between TCP and UDP: • TCP - ACOS maintains a session and retains the TCP connection to the server alive. • UDP - Only the ACOS session is kept alive. no UDP traffic is sent back and forth to the server unless there is a DNS query to be forwarded to the server. **NOTE:** **`source-nat`** must be enabled with **`auto`** or **`pool`** option inside the DoH template.
`dns-retry`	Specify the retry policy in the DNS over HTTP(s) template. The dns-retry parameters are only applicable for DNS server-side traffic based on UDP. This command enters the dns-retry configuration mode where the following options are available: • **`after-timeout {close | retry-with-tcp}`**: Action to take after timeout. ◦ `close`: Close client-side connection. This is the default option.

Command	Description
	◦ `retry-with-tcp`: ACOS connects to a backend DNS server with TCP servers configured using the **`tcp-service-group`** command. When a backend UDP based DNS server responds with a DNS response with TC (truncation) bit set, ACOS retries to connect to same server using DNS over TCP and does not use the **`tcp-service-group`** to select a new server. • **`max-trials <1-5>`**: Total number of times to try DNS query to server before closing client connection. Default value is 3. • **`retry-interval <1-400>`**: DNS Retry Interval value 1 to 400 in units of 100ms. Default is 10(1000ms).
`forwarder`	Specify the DNS over HTTP(s) template forwarding policy. This command enters the DNS over HTTP(s) forwarding policy mode where the following options are available: • **`bypass-doh`** - When this command is configured, the HTTP request is forwarded to the service-group as is after the DNS template validates the DNS query. This way, DoH forwarding is bypassed for valid DoH request. **Note:** This command is mutually exclusive to the service groups or other forwarding commands. • **`forwarding-ipv4`** *`<ipv4 address>`*: This IPv4 can be used to forward the traffic externally or internally to another VIP. • **`forwarding-ipv6`***`<ipv6 address>`*: This IPv6 can be used to forward the traffic externally or internally to another VIP. • **`tcp-service-group`** *`<tcp_sg_name>`*: Bind a TCP

Command	Description
	Service Group to the template. • **udp-service-group** *<udp_sg_name>*: Bind a UDP Service Group to the template. **Note:** • You can configure either **udp-service-group** or **tcp-service-group** or both. • When only one type of service-group is configured, ACOS will use that for DNS load balancing. • When both types of service-groups (TCP as well as UDP) are configured, ACOS will by default, use the UDP service-group. TCP service-group will be used, only if the UDP servers are not reachable and the **after-timeout retry-with-tcp** command is configured under **dns-retry** parameter. Additionally, you can also set either or all the below parameters along with the `tcp`, `udp` or `both` the protocols: • *internal*: Set this to find the IP (v4/v6) as a VIP in this L3V partition and forward it internally to the VIP. • *port*: Set this to forward to a port number. By default, the port is 53. • *protocol*: Set this for Layer 4 protocol type. By default, the protocol is `both`.
non-dns-request {allow | reject [400 | 500 | 501]}	Specify any one of the actions for non DNS request: • **allow**: allow request • **reject**: deny request with the following status codes: ◦ 400 Status Code 400 BAD Request (Default)

Command	Description
	◦ 500 Status Code 500 Internal Server Error ◦ 501 Status Code 501 Not Implemented
source-nat	Specify the action to enable or disable Source NAT. Default is Source NAT Auto with the sub-options: • **auto**: Perform Source NAT Auto (Default). • **disable**: Disable Source NAT for server side DNS queries. "conn-reuse" is not supported when **source-nat** is "disabled" • **pool**: Perform Source NAT with specific pool.
template	Specify one of the options to apply to the DoH template: • **dns <dns template name>** - Apply a DNS template to the DoH template. • **tcp-proxy <tcp-proxy template name>** - Apply a TCP-proxy template to the DoH template. **Note:** This template configuration is applicable to DNS over TCP server side traffic only.

Mode Global Configuration Mode

Usage You can bind only one DoH template to a virtual port. However, you can bind the same DoH template to multiple ports.

DoH templates are not supported with stateless load-balancing methods.

Example The following example configures a new DoH template and enables connection reuse:

```
ACOS(config)# slb template doh doh1
ACOS(config-doh)# conn-reuse enable
```

Example The following example configures a new DoH template and sets IPv4 address forwarding policy internally with TCP protocol:

```
ACOS(config)# slb template doh doh2
ACOS(config-doh)# forwarder
ACOS(config-doh-forwarder)# forwarding-ipv4 10.10.1.10
internal port 53 protocol tcp
```

Example The following example configures a new DoH template and sets IPv4 address forwarding policy to external DNS server:

```
ACOS(config)# slb template doh doh3
ACOS(config-doh)# forwarder
ACOS(config-doh-forwarder)# forwarding-ipv4 10.23.1.1
```

See Also:

- Application Delivery Controller Guide

slb template dynamic-service

Description Creates a template that you can bind to virtual ports to access specific DNS servers.

Syntax

```
[no] slb template dynamic-service template-name
```

This command changes the CLI mode to dynamic service configuration mode, where the following commands are available:

Command	Description
class-list *string* **priority**{ **dns server**}	Configure Aho-Corasick (AC) class-list for specific destination domains. You can configure a maximum of 64 class-lists. **priority** *1-64*: Specify a priority for the configured class-list. The value can be from 1-64. The larger number has the higher priority. **dns server** *{ipv4- address | ipv6 address}*: Specify the DNS server's IP address (IPv4 or IPV6) for the specified class-list. When the requested domain name matches the class-list, ACOS uses the DNS server configured with the class-list.

Command	Description
	The class-list can contain a maximum of two DNS server IP addresses.
dns server *dns-ip-address*	Specify a maximum of two DNS servers. These are considered as default DNS servers.

Default No default template

Mode Global Configuration mode

Usage Creates a dynamic service template to bind virtual ports for providing DNS resolution while forwarding traffic to the internet. You can create a maximum of two default DNS servers and 64 class-lists with two DNS servers and specified domain names.

The traffic is forwarded based on the following workflow:

1. If the class-list and the corresponding DNS server are configured in the dynamic-service template, then ACOS selects the DNS server based on the domain name of the request. If the domain name matches one of the class-list, the corresponding DNS server is selected. If the domain name matches multiple class-lists, the class-list is selected based on the priority set.
2. If the class-list and the corresponding DNS server are not set, then ACOS checks the configuration of the default DNS server set in the dynamic service template. If the default server is set, ACOS selects the default server to resolve IP address.
3. If both the class-list and the default DNS servers are not configured, then ACOS checks the configuration of the Global DNS server in the **ip dns <primary/secondary>** command.

Example The following example creates the dynamic-service template `dns_service1` , which has a class-list with a defined priority and DNS servers. The template is bound to the HTTPS virtual port of `Inside_VIP` virtual server.

```
ACOS(config)# slb template dynamic-service dns_service1
ACOS(config-dynamic-service)#class-list test1 priority 20
ACOS(config-dynamic-service-class-list)# dns server 1.1.1.1
ACOS(config-dynamic-service-class-list)# dns server 2.2.2.2
```

```
ACOS(config-dynamic-service)# exit
```

```
ACOS-Inside(config)# slb virtual-server Inside_VIP 10.10.1.30
ACOS-Inside(config-slb vserver)# port 443 https
ACOS-Inside(config-slb vserver-vport)# service-group FW1_
Inspect_SG
ACOS-Inside(config-slb vserver-vport)# template client-ssl
SSLInsight_ClientSide
ACOS-Inside(config-slb vserver-vport)# template policy
Explicit_Proxy
ACOS-Inside(config-slb vserver-vport)# template dynamic-
service dns_service1
```

Related Commands

- class-list

slb template external-service

Description Configure an External Service template to steer traffic to external servers for additional processing, based on application.

NOTE: This command is not supported for HTTP/2 virtual port.

Syntax

```
[no] slb template external-service template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB External-Service Template Configuration mode where the following commands are available.

Command	Description
[no] **bypass-ip** *IPv4-address* {**/***nn* |	If configuring for ICAP-based Traffic Steering, specifies the controller IP address.

Command	Description
netmask}	
[**no**] **failure-action** {**continue** | **drop** | **reset**}	Specifies the action performed by ACOS when any of the following types of events occurs: • ACOS fails to select an external-service server. • Failure during creation of a new connection to external-service server. • The response from the external-service server does not contain HTTP status code 200 or 403. • Exhaustion of memory when creating a request to external-service server. The failure action can be one of the following: • **continue** – Allows the client's request to go to the content server. • **drop** – Silently drops connection and does not send a reset to the client. • **reset** – Sends a connection reset to the client. **NOTE:** If a TCP error occurs while ACOS is waiting for a response, ACOS resets the connection. For example, this occurs in the case of a connection reset by a URL filtering server. The default is **continue**.
[**no**] **request-header-forward** *header-name*	Enable forwarding of additional headers to the proxy server. If there are multiple headers with the same name from the client, then only the first header instance will be forwarded. The URL Filter server's HTTP module parses the client request and saves the results in the corresponding data structure. ACOS then inserts the configured

Command	Description
	header when it forwards the HTTP request to the proxy server. If the response from the proxy server is good, then ACOS connects to the destination server. If the response from the proxy server is bad, then ACOS closes the connection. Only GET and POST methods are forwarded by the SLB "external-service" template, so only these methods will forward the configured request-headers to the proxy servers. A maximum of 16 HTTP headers can be forwarded. One HTTP header only can be 1036 bytes, including the HTTP header name and HTTP header element. Anything longer than that will be truncated at 1036 bytes. If there are multiple headers with the same name from the client, then only the first header instance will be forwarded. This is not enabled by default.
[**no**] **service-group** *group-name*	Binds the service group that contains the external-service servers to this template. Specify the service group that contains the external-service servers (for example, ICAP-based Traffic Steering servers or URL-filtering servers). Do not specify the service group containing the content servers (HTTP servers). If configuring for ICAP-based Traffic Steering, specify the group of servers here, but not the controller. Specify the controller using the **bypass-ip** command (described below)
[**no**] **template** *template-type*	Applies a template to the external-service template. Specify one or both of the following: • **persist source-ip** *template-name* – Applies a

Command	Description
template-name	source-IP persistence template to the external-service template. • **tcp-proxy** *template-name* – Applies a custom TCP-proxy template to use for managing the TCP connections with the servers.
[**no**] **timeout** *num* **action** [**continue** | **drop** | **reset**]	Sets the maximum number of seconds ACOS waits for a response from the server. If the server does not reply before the timeout expires, ACOS takes the configured action, which can be one of the following: • **continue** – Allows the client's request to go to the content server. • **drop** – ACOS silently drops the connection and does not send a reset to the client. • **reset** – ACOS sends a connection reset to the client. The default is 1000ms, **continue**.
[**no**] **type** [**skyfire-icap** | **url-filter**]	Specifies the traffic type to redirect: • **skyfire-icap** – Steers Internet Content Adaptation Protocol (ICAP) to external controllers. • **url-filter** – Steers HTTP requests from clients to external URL-filtering servers. The default is **url-filter**.

Default No default External Service template.

Mode Global Configuration mode

Example The following command configures the External Service template **service1** to steer traffic to Skyfire ICAP server.

```
ACOS(config)#slb template external-service service1
ACOS(config-external-service)#type skyfire-icap
```

slb template fix

Description Configure a template for Financial Information Exchange (FIX) load balancing.

Syntax

```
[no] slb template fix template-name
```

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters the SLB FIX Template Configuration mode where the following commands are available.

Command	Description
[no] insert-client-ip	Inserts an AVP with the original client IP address to the tag 11447. For example, if the client IP address is 40.40.40.20, this option will modify the tag to "11447=40.40.40.20" when the server receives this client's PUSH data.
logging	Enables logging of messages. The following options can be configured for logging: • `init` - Logs only the initial log. • `term` - Logs only the termination log. • `both` - Logs both initial and termination log.
[no] tag-switching [sender-comp-id | target-comp-id] equals *string* **service-group** *name*	Inspects the FIX message header for a SenderCompID or TargetCompID tag value and uses a specific service group if the tag matches the Equals keyword. The ACOS device can inspect FIX messages and perform service group switching with one of the following options: • **sender-comp-id** – Selects a service group for FIX requests based on the value of the SenderCompID tag. This tag identifies the financial institution that is sending the request. • **target-comp-id** – Selects a service group for FIX

Command	Description
	requests based on the value of the TargetCompID tag. This tag identifies the financial institution to which the request is being sent. If you select the Sender Comp ID or Target Comp ID radio button, the following options are displayed: • **equals** *string* – Specifies a keyword which ACOS matches against the TargetCompID or SenderCompID tag of a FIX message header. **NOTE:** The keyword is case sensitive and must match exactly with the SendCompID tag or TargetCompID tag. For example, "ABC" is different from "Abc". • **service-group** *name* – Selects the service-group to use for a client request when the SenderCompID or TargetCompID tag in the FIX message header of the request matches the specified keyword.

Default No default FIX template.

Mode Global Configuration mode

Example The following example configures the `fix1` slb FIX template and enables logging of initial logs related to SLB FIX template.

```
ACOS(config)##slb template fix fix1
ACOS(config-fix)#logging init
```

slb template ftp

Description Configure a template for FTP load balancing.

Syntax

```
[no] slb template ftp template-name
```

Replace *template-name* with the name of the template, 1-127 characters long.

This command enters the SLB FTP Template Configuration mode where the following commands are available.

Command	Description
[no] **active-mode-port** *num* **to** *num*	Provide a non-standard FTP active mode port number. • *num* - Specify a port number in the range 1 to 65534. • **any** - Allow any FTP Active mode port.

Default No default FTP template.

Mode Global Configuration mode

Example The following command configures the ftp1 template and specifies the non-standard FTP active mode port range.

```
ACOS(config)#slb template ftp ftp1
ACOS(config-ftp template)#active-mode-port 1012 to 2020
```

slb template http

Description Configure HTTP modifications to server replies to clients and configure load balancing based on HTTP information.

Syntax

```
[no] slb template http template-name
```

Replace *template-name* with the name of the template, up to 31 characters.

This command enters the SLB HTTP Template Configuration mode where the following commands are available.

Command	Description
[no] 100-cont-wait-	When the server receives an HTTP Post request with an Expect:100 Continue, it considers all

Command	Description
for-req-complete	subsequent inbound packets as belonging to the request until it receives the expected number of packets for the request.
[no] allowed-methods	Allows to configure HTTP methods that are permitted by the system (GET, BIND, CONNECT, COPY, DELETE, HEAD, LABEL, LOCK, MERGE, MKCOL, MOVE, OPTIONS, PATCH, POST, PRI, PROPFIND, PROPPATCH, PUT, REBIND, TRACE, UNBIND, UNLINK, UNLOCK, UPDATE, PURGE, and TRACK). • **action**- Specify the 'drop' action. If this option is not configured, the traffic will not be dropped even it matches the combinations.
client-idle-timeout *seconds*	Specifies the number of seconds the client connection can be idle before the ACOS device terminates the connection. The range is 0-120 seconds. By default, the value is 0 seconds i.e. it is disabled. This option is supported only for HTTP, HTTPS, and HTTP/2 virtual port types. It is not supported on fast-HTTP or other virtual port types.
[**no**] **compression** *option*	Offloads Web servers from CPU-intensive HTTP compression operations. The following are the sub-options for this command:
	auto-disable-on-high-cpu *percent* Configures an automatic disable of HTTP compression based on CPU utilization. The *percent* option specifies the threshold. You can specify 1-100.
	brotli-level *number* Specifies the brotli compression level. The

Command	Description
	compression level can be between 1-9. The default level is 1. Where, • level 1 provides the lowest compression ratio. • level 9 provides the higher compression ratio. A higher compression ratio results in a smaller file size after compression. However, higher compression levels also require more CPU processing than lower compression levels, so performance can be affected. Compression is supported for HTTP/2 and HTTP 1.1 protocols, if the **method-order** is specified.
	brotli-sliding-window *number* Specify the LZ77 value ('lgwin' of 'brotli') of the brotli window size. The header contains the size of the sliding window that is used during compression. The range of 10 to 24 means the possible sliding window sizes ranges from 1KiB-16 to 16MiB-16. 10 Means 1KiB-16. The default value is 10. Consider the following points while setting this value: • A larger sliding window size will tend to have a higher compression ratio compared with the one with smaller size when the distance between the consecutive similar patterns are far away. • A smaller sliding window size will lower the CPU workload as it only scans a smaller number of

Command	Description
	bytes for a match.
	content-type *content-string* Specifies type of content to compress, based on a string in the content-type header of the HTTP response. The *content-string* can be 1-31 characters long. The “text” and “application” types are included by default.
	enable Enables compression.
	exclude-content-type *content-string* Excludes the specified content type from being compressed. The *content-string* can be 1-31 characters long.
	exclude-uri *uri-string* Excludes an individual URI from being compressed. The URI string can be 1-31 characters. An HTTP template can exclude up to 10 URI strings.
	keep-accept-encoding enable Configures the ACOS device to leave the Accept-Encoding header in HTTP requests from clients instead of removing the header. When keep-accept-encoding is enabled, compression is performed by the real server instead of the ACOS device, if the server is configured to perform the compression. The ACOS device compresses the content that the real server does not compress. This option is disabled by

Command	Description
	default, which means the ACOS device performs all the compression. This is disabled by default.
	level *number* Specifies gzip compression level. The compression level can be between 1-9. The default level is 1. Where, • level 1 provides the lowest compression ratio. • level 9 provides the higher compression ratio. A higher compression ratio results in a smaller file size after compression. However, higher compression levels also require more CPU processing than lower compression levels, so performance can be affected. Compression is supported for HTTP, HTTPS, and HTTP/2 virtual ports. **NOTE:** Compression is not supported for fast-HTTP virtual ports.
	method-order *string* Specify the order of compression algorithm to be applied when multiple compression algorithms are included in the (**accept-encoding**) request HTTP header. For example, if "gzip brotli" is configured, then gzip will be used when both 'gzip' and 'Brotli' are acceptable.

Command	Description
	NOTE: This option must be configured when the brotli-related commands are configured and compression must be enabled (**enable**).
	minimum-content-length *bytes* Specifies the minimum length (in bytes) a server response can be in order to be compressed. The length applies to the content (payload) only and does not include the headers. You can specify 0-2147483647 bytes. The default is 120 bytes.
[**no**] **cookie-format rfc6265**	Configures the HTTP cookie parser to supports RFC 6265. By default, the HTTP cookie parser is compliant only with RFC 2109 and RFC 2965.
[no] default-charset	Set the default charset to decode HTTP body if the charset cannot be determined by other methods. The default is UTF-8.
[no] disallowed-methods	Blocks HTTP methods that are restricted by the system to protect web applications. • **action**- Specify the 'drop' action. If this option is not configured, the traffic will not be dropped even it matches the combinations.
[**no**] **failover-url** *url-string*	Specifies the fallback URL to send in an HTTP 302 response when all real servers are down.
[no]frame-limit*number <0-65535>*	Specifies the control frame limit for specific frame elements per connection. It limits the number of CONTINUATION, PING, PRIORITY, RESET, SETTINGS and empty frames that can be sent in one HTTP2 connection. The default is 10000. If the limit is exceeded, the

Command	Description
	connection is reset.
[**no**] **host-switching** {**starts-with** | **contains** | **regex-match** **ends-with**} *host-string* **service-group** *service-group-name*	Selects a service group based on the value in the Host field of the HTTP header. The selection overrides the service group configured on the virtual port. For *host-string*, you can specify an IP address or a hostname. If the host-string does not match, the service group configured on the virtual port is used. • **starts-with** *host-string* – matches only if the hostname or IP address starts with *host-string*. • **contains** *host-string* – matches if the *host-string* appears anywhere within the hostname or host IP address. • **regex-match** *host-string* – matches if the *host-string* matches the hostname or host IP address. • **ends-with** *host-string* – matches only if the hostname or IP address ends with *host-string*. **NOTE:** You can use URL switching *or* Host switching in an HTTP template, but not both. However, if you need to use both types of switching, you can do so with an aFleX script.
[**no**] **http-protocol-check** *options*	Enables the HTTP protocol compliance check and drops the request based on the configured options (as given below). ACOS will respond 400 to the client-side and then discard the request. The following options are available in this

Command	Description
	command:
	get-and-payload *drop* Configures the drop action if the HTTP/1 or HTTP/2 request has a GET method and Transfer-Encoding (TE) or Content-Length (CL) header simultaneously.
	h2up-content-length-alias *drop* Configures the drop action if the content-length/content_length header appears in the HTTP/2 request.
	h2up-with-host-and-auth *drop* Configures the drop action if the HTTP/2 request has both host header and :authority pseudo header.
	h2up-with-transfer-encoding *drop* Configures the drop action if the HTTP/2 request includes the TE header.
	header-filter-rule *seq-num* {**action** | **header-name** | **header-value** | **match-type** | **user-tag**} Configures the filter rules to the HTTP headers content and apply the specified action. The traffic is filtered or dropped as per the defined rules. The following options must be explicitly specified: • **action** - Specify the 'drop' action. If this option is not configured, then the traffic will not be dropped even if it matches the filter rules. • **header-name** - Specify the regular expression or full-text of the header-name based on the match-type. • **header-value** - Specify the regular expression or

Command	Description
	full-text of the header-value based on the match-type. • **match-type** - Specify the regular expression filter string to match. The match-type can be either 'full-text' or 'PCRE' compatible regular expressions. For information about PCRE-compatible regular expressions, see official Perl Documentation. **NOTE:** The match-type option must be configured before the header-name and header-value. The action option can be configured after the header-name and header-value. You can configure a maximum of five filter rules. When more than one rule matches an HTTP request, the rule with the lower sequence number is executed first. As a result, the lower the sequence number higher the priority when this condition occurs. • **user-tag** *name* - Configures the customized tag.
	malformed-h2up-header-value *drop* Configures the drop action if the header value of the HTTP/2 request includes \r or \n.
	malformed-h2up-scheme-value *drop* Configures the drop action if the scheme value of the HTTP/2 request is not HTTP/HTTPS.
	multiple-content-length *drop* Configures the drop action if the HTTP/1 or HTTP/2 request has multiple CL headers.
	multiple-transfer-encoding *drop*

Command	Description
	Configures the drop action if the HTTP/1 or HTTP/2 request has multiple TE headers.
	transfer-encoding-and-content-length *drop* Configures the drop action if the HTTP/1 or HTTP/2 request has both the CL and TE headers.
http2-client-no-snat	Enable this option to dynamically adjust the max-concurrent-stream value when the source NAT is not configured under the virtual port, and the client-side is HTTP2, and the server-side is HTTP1. The max-concurrent-streams will be set to '1' until the server supports HTTP2 and accepts other values.
[**no**] **insert-client-ip** [*http-header-name*] [**replace**]	Inserts the client's source IP address into HTTP headers. If you specify an HTTP header name, the source address is inserted only into headers with that name. The **replace** option replaces any client addresses that are already in the header. Without this option, the client IP address is appended to the lists of client IP addresses already in the header. For example, if the header already contains "X-Forwarded-For:1.1.1.1" and the current client's IP address is 2.2.2.2, the **replace** option changes the *field*:*value* pair to "X-Forwarded-For:2.2.2.2". Without the **replace** option, the *field*:*value* pair becomes "X-Forwarded-For:1.1.1.1, 2.2.2.2".
[**no**] **insert-client-port** [*http-header-name*] [**replace**]	Inserts the source protocol port of the client's request into the HTTP header. If no header name is specified, the X-ClientPort header is used. The **replace** option allows you to replace the content of an existing header that matches the

Command	Description
	configured name with the client's port number. If no header name is specified, the X-ClientPort header is used. If the **replace** option is not specified, and there is a header that matches the configured name, the client's port number is added to the end of the specified header.
[**no**] **keep-client-alive**	Keeps the session between ACOS and the session up even after the part of the session between ACOS and the backend server is terminated.
[**no**] **log-retry**	Logs HTTP retries. An HTTP retry occurs when the ACOS device resends a client's HTTP request to a server because the server did not reply to the first request. (HTTP retries are enabled using the **retry-on-5xx** or **retry-on-5xx-per-req** command in the HTTP template.)
[**no**] **max-con-current-streams**	Set the maximum concurrent streams for HTTP2 only. The value can be between 1-1000 and the default value is 100.
[**no**] **non-http-bypass service-group** *group-name*	Redirects non-HTTP traffic to a specific service group. By default, the ACOS device will drop non-HTTP requests that are sent to an HTTP port.
[**no**] **persist-on-401**	Enable this option to persist on the same server if the HTTP response code is 401.
[**no**] **redirect [location** *location*| **port** *portnum* | **response-code** |**secure]**	Automatically sends a redirect response to HTTP client requests. You can optionally specify the following: • **location** *location* A static location string to which the client will be redirected.

Command	Description
	• **port** *portnum* TCP port number to use for the redirect. • **response-code** The response code to apply. 302 Found is used by default. The following response codes can be configured: ◦ 301 (Moved Permanently) ◦ 302 (Found) ◦ 303 (See Other) ◦ 307 (Temporary Redirect) • **secure** The client will be redirected using HTTPS.
[**no**] **redirect-rewrite match** *url-string* **rewrite-to** *url-string*	Modifies redirects sent by servers by rewriting the matching URL string to the specified value before sending the redirects to clients.
[**no**] **redirect-rewrite secure** {**port** *tcp-portnum*}	Changes HTTP redirects sent by servers into HTTPS redirects before sending the redirects to clients. To redirect clients to the default HTTPS port (443), enter the following command: **redirect-rewrite secure** To redirect clients to an HTTPS port other than the default, enter the following command instead: **redirect-rewrite secure port** *port-num*
[**no**] **req-hdr-wait-time**	Sets a request header wait time to prevent

Command	Description
seconds	Slowloris attacks. All portions of a client's request header must be received within the specified amount of time. Otherwise, ACOS terminates the connection. You can specify 1-31 seconds. The default is 7.
[**no**] **request-header-erase** *field*	Erases the specified header (field) from HTTP requests.
[**no**] **request-header-insert** *field*:*value* [**insert-always** | **insert-if-not-exist**]	Inserts the specified header into HTTP requests. The *field*:*value* pair indicates the header field name and the value to insert. • If you use the **insert-always** option, the command always inserts the *field:value* pair. If the request already contains a header with the same *field* name, the new *field:value* pair is added after the existing *field:value* pair. Existing headers are not replaced. • If you use the **insert-if-not-exist** option, the command inserts the header only if the request does not already contain a header with the same *field* name. Without either option, if a request already contains one or more headers with the specified *field* name, the command replaces the last header.
[**no**] **request-line-case-insensitive**	Parses HTTP request lines with no case sensitivity.
[**no**] **request-timeout**	Requests a timeout in seconds if there is no response from the server. The range is 1 to 120 seconds.

Command	Description
	This option is supported only on virtual port types HTTP and HTTPS. It is not supported on fast-HTTP or other virtual port types.
[**no**] **response-content-replace** *original-content new-content*	Replaces data in the HTTP response from the server. The *original-content* specifies the content to look for in server responses. The *new-content* specifies the content to use to replace the original content. For each value, you can specify a string of 1-127 characters. If a string contains blank spaces, use double quotation marks around the string. **NOTE:** A maximum of 8 content-replacement rules are supported in a given HTTP template.
[**no**] **response-header-erase** *field*	Erases the specified header (field) from HTTP responses.
[**no**] **response-header-insert** *field*:*value* [**insert-always** | **insert-if-not-exist**]	Inserts the specified header into HTTP responses. The *field:value* pair indicates the header field name and the value to insert. • If you use the **insert-always** option, the command always inserts the *field:value* pair. If the response already contains a header with the same *field* name, the new *field:value* pair is added after the existing *field:value* pair. Existing headers are not replaced. • If you use the **insert-if-not-exist** option, the command inserts the header only if the response does not already contain a header with the same *field* name. Without either option, if a response already contains one or more headers with the specified

Command	Description
	field name, the command replaces the first header.
[no] **retry-on-5xx** *num*	Configures the ACOS device to retry sending a client's request to a service port that replies with an HTTP 5xx status code, and reassign the request to another server if the first server replies with a 5xx status code. The retry number specifies the number of times the ACOS device is allowed to reassign the request. For example, assume that a service group has three members (s1, s2, and s3), and the retry is set to 1. In this case, if s1 replies with a 5xx status code, the ACOS device reassigns the request to s2. If s2 also responds with a 5xx status code, the ACOS device will not reassign the request to s3, because the maximum number of retries has already been used.
[no] **retry-on-5xx** *num* *(cont)*	If you use this command, the ACOS device stops sending client requests to a service port for 30 seconds following reassignment. If you want the service port to remain eligible for client requests, use the following command instead. An HTTP template can contain one or the other of these commands, but not both. **NOTE:** The 5xx options are supported for virtual port types HTTP, HTTPS and HTTP/2. They are not supported for fast-HTTP or any other virtual port type.
[no] **retry-on-5xx-per-req** *num*	This command provides the same function as the **retry-on-5xx** command (described above). However, the **retry-on-5xx-per-req** command does not briefly stop using a service port following reassignment. An HTTP template can contain one

Command	Description
	or the other of these commands, but not both.
[**no**] **strict-transaction-switch**	Forces the ACOS device to perform the server selection process anew for every HTTP request. Without this option, the ACOS device reselects the same server for subsequent requests (assuming the same server group is used), unless overridden by other template options.
[**no**] **template logging** *template-name*	Specifies a logging template to use for external logging of HTTP events over TCP.
[**no**] **term-11client-hdr-conn-close**	Enables the ACOS device to terminate HTTP 1.1 client connections when the "Connection: close" header exists in the HTTP request. This option is applicable to connection-reuse deployments that have HTTP 1.1 clients that are not compliant with the HTTP 1.1 standard. Without this option, sessions for non-compliant HTTP 1.1. clients are not terminated.
[**no**] **url-hash-persist** [**offset** *offset-bytes*] {**first** | **last**} *bytes* [**user-server-status**]	Enables server stickiness based on hash values. If this feature is configured, for each URL request, the ACOS device calculates a hash value based on part of the URL string. The ACOS device then selects a real server based on the hash value. A given hash value always results in selection of the same real server. Thus, requests for a given URL always go to the same real server. The **offset** option specifies how far into the string to begin hash calculation. The **first** and **last** options specify which end of the URL string to use to calculate the hash value. The *bytes* option specifies how many bytes to use to calculate the hash value.

Command	Description
	Optionally, you can use URL hashing with either URL switching or host switching. Without URL switching or host switching configured, URL hash switching uses the hash value to choose a server within the default service group (the one bound to the virtual port). If URL switching or host switching is configured, for each HTTP request, the ACOS device first selects a service group based on the URL or host switching values, then calculates the hash value and uses it to choose a server within the selected service group. The **use-server-status** option enables server load awareness, which allows servers to act as backups to other servers, based on server load. **NOTE:** This feature requires some custom configuration on the server. For information, see the "URL Hash Switching" section in the "HTTP Options for SLB" chapter of the *Application Delivery Controller Guide*.
[no] **url-switching** {**starts-with** | **ends-with** | **regex-match** **url-case-insensitive** | **url-hits-enable**} *url-string* **service-group** *service-group-name*	Selects a service group based on the URL string requested by the client. The selection overrides the service group configured on the virtual port. • **starts-with** – matches only if the URL starts with *url-string*. • **contains** – matches if *url-string* appears anywhere within the URL. • **ends-with** – matches only if the URL ends with *url-string*. • **regex-match** – matches if the URL matches *url-string*.

Command	Description
	• **url-case-insensitive** – enable case-insensitive matching for URL switching rules. • **url-hits-enable** – enable URL hits. Each URL matching pattern can be up to 64 bytes long. **NOTE:** You can use URL switching *or* Host switching in an HTTP template, but not both. However, if you need to use both types of switching, you can do so with an aFleX script.

NOTE: The order in which **content-type**, **exclude-content-type**, and **exclude-uri** filters appear in the configuration does not matter.

Default The configuration has a default HTTP template. In the template, most options are disabled or not set.

To display the default HTTP template settings, use the **show slb template http default** command.

Mode Configuration mode

Usage The normal form of this command creates an HTTP configuration template. The **no** form of this command removes the template.

You can bind only one HTTP template to a virtual port. However, you can bind the same HTTP template to multiple ports.

Header insertion is not supported on fast-HTTP virtual ports.

When the **keep-client-alive** option is enabled, the way ACOS keeps the session with the client up depends on the way the server session is terminated:

- Normal TCP/IP connection termination by a TCP RST or FIN – ACOS does not forward the RST or FIN to the client, and instead leaves the client session open. (Technically, the session is left in the client-request-state, wherein ACOS awaits the client's next request.)

- "Connection: Close" header option in the response – ACOS removes this header from the server reply before forwarding the reply to the client.
- Client is using HTTP 1.0, and did not use the "Connection: Keep-Alive" header option – ACOS inserts this header from the server reply before forwarding the reply to the client.

Starts-with, Contains, and Ends-with Rule Matching

The **starts-with**, **contains**, and **ends-with** options are always applied in the following order, regardless of the order in which the commands appear in the configuration. The service group for the first match is used.

- starts-with
- contains
- ends-with

If a template has more than one command with the same option (**starts-with**, **contains**, or **ends-with**) and a host name or URL matches on more than one of them, the most-specific match is always used. For example, if a template has the following commands, host "ddeeff" will always be directed to service group http-sgf:

```
slb template http http-host
  host-switching starts-with d service-group http-sgd
  host-switching starts-with dd service-group http-sge
  host-switching starts-with dde service-group http-sgf
```

If a **contains** rule and an **ends-with** rule match on exactly the same string, the **ends-with** rule is used, because it has the more specific match.

If you use the **starts-with** option with URL switching, use a slash in front of the URL string. For example:

```
  url-switching starts-with /urlexample service-group http-sg1
```

Redirect-Rewrite Rule Matching

If a URL matches on more than redirect-rewrite rule within the same HTTP template, the ACOS device selects the rule that has the most specific match to the URL. For example, if a server sends redirect URL

66.1.1.222/000.html, and the HTTP template has the redirect-rewrite rules shown below, the ACOS device will use the last rule because it is the most specific match to the URL:

```
slb template http 1
   redirect-rewrite match /00 rewrite-to http://66.1.1.202/a
   redirect-rewrite match /000.html rewrite-to /001.gif
   redirect-rewrite match 66.1.1.222/000.html rewrite-to
66.1.1.202/003.bmp
```

Example The following commands configure an HTTP template called “http-compression” that enables compression. The minimum length a packet must be for it to be compressed is set at 120 bytes.

```
ACOS(config)# slb template http http-compression
ACOS(config-http)# compression enable
ACOS(config-http)# compression minimum-content-length 120
```

Example The following commands configure an HTTP template called “http-header” that inserts the client IP address and a Cookie field into HTTP headers in requests from clients before sending the requests to servers:

```
ACOS(config)# slb template http http-header
ACOS(config-http)# insert-client-ip
ACOS(config-http)# header-insert Cookie:a = b
```

Example The following commands configure an HTTP template called “http-host” that selects a service group based on the contents of the Host field in the HTTP headers of client requests. Requests for hostnames that start with “Gossip” are directed to service group “http-sg1”. Requests for hostnames that contain “NewsDeskA” are directed to service group “http-sg2”. Requests for hostnames that end with “weather.com” are directed to service group “http-sg3”.

```
ACOS(config)# slb template http http-host
ACOS(config-http)# host-switching starts-with Gossip service-
group http-sg1
ACOS(config-http)# host-switching contains NewsDeskA service-
group http-sg2
ACOS(config-http)# host-switching ends-with weather.com
service-group http-sg3
```

Example These commands configure an HTTP template to use URL hashing. Hash values are calculated based on the last 8 bytes of the URL. In this example, URL switching is also configured in the template. As a result, the ACOS device uses URL switching to select a service group first, then uses URL hashing to select a server within that service group. If the template did not also contain URL switching commands, this template would always select a server from service group sg3.

```
ACOS(config)# slb template http hash
ACOS(config-http)# url-hash-persist last 8
ACOS(config-http)# url-switching starts-with /news service-
group sg1
ACOS(config-http)# url-switching starts-with /sports service-
group sg2
ACOS(config-http)# exit
ACOS(config)# slb virtual-server vs1 1.1.1.1
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# service-group sg3
ACOS(config-slb vserver-vport)# template http hash
```

Example These commands configure an HTTP template called “http-compress”, that uses compression level 5 to compress files with media type “application” or “image”. Files with media type “application/zip” are explicitly excluded from compression.

NOTE: For a list of media type strings, see the Internet Assigned Numbers Authority Web site: http://www.iana.org/assignments/media-types.

```
ACOS(config)# slb template http http-compress
ACOS(config-http)# compression enable
ACOS(config-http)# compression level 5
ACOS(config-http)# compression content-type image
ACOS(config-http)# compression exclude-content-type
application/zip
```

Example These commands configure an HTTP template that replaces the client IP addresses in the X-Forwarded-For field with the current client IP address:

```
ACOS(config)# slb template http clientip-replace
ACOS(config-http)# insert-client-ip X-Forwarded-For replace
```

Example These commands enter slb-port template configuration mode for the port name xyz, then configures that port, upon receiving an HTTP request with an Expect: 100 Continue, assigns all subsequent packets to that request until it receives an expected number of packets.

```
ACOS(config)# slb template http abc
ACOS(config-http)# 100-cont-wait-for-req-complete
```

Example These commands configure an HTTP template that enables brotli compression algorithm:

```
ACOS(config)# slb template http http_brotli
ACOS(config-http)# compression enable
ACOS(config-http)# compression brotli-level 5
ACOS(config-http)# compression brotli-sliding-window 2
ACOS(config-http)# compression method-order "gzip brotli"
```

Example These commands configure an HTTP template with the HTTP protocol compliance check:

```
ACOS(config)# slb template http abc
ACOS(config-http)# http-protocol-check
ACOS(config-http-http-protocol-check)# h2up-content-length-
alias drop
ACOS(config-http-http-protocol-check)# malformed-h2up-header-
value drop
```

Example These commands configure the HTTP header filter rules under HTTP protocol compliance.

```
ACOS(config)# slb template http abc
ACOS(config-http)# http-protocol-check
ACOS(config-http-http-protocol-check)# header-filter-rule
ACOS(config-http-http-protocol-check-head...)# match-type
full-text
ACOS(config-http-http-protocol-check-head...)# action drop
ACOS(config-http-http-protocol-check-head...)# header-name
content-encoding
ACOS(config-http-http-protocol-check-head...)# header-value
chunked
```

slb template http-policy

Description Configures an HTTP-policy template and allows server selection for different types of client traffic.

Syntax

```
[no] slb template http-policy  template-name
```

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters the SLB HTTP-Policy Template Configuration mode where the following commands are available.

Command	Description
[**no**] **cookie-name** *cookie-name*	Matches the cookie-name first and then matches the cookie value. The value in this command is case-sensitive.
[**no**] **cookie** *match-option URL string* {**service-group** *group-name*}	Matches based on cookie values. Descriptions of the match-options are mentioned below: • `contains` - Matches if the specified string appears anywhere within the cookie value. • `ends-with` - Matches only if the cookie value ends with the specified string. • `equals` - Matches only if the cookie value completely matches the specified string • `starts-with` - Matches only if the cookie value starts with the specified string. The value in this command is case-sensitive.
[**no**] **geo-location** *string* {**service-group** *group-name*}	Matches the traffic source based on its geo-location. This condition type is not supported for the **multi-match-rule**.
	Matches based on the name of the header. Descriptions of the match-options are

Command	Description
[no] header-name *match-option string* {**service-group** *service-group-name*}	mentioned below: • `contains` - Matches if the specified string appears anywhere within the header name. • `ends-with` - Matches only if the header name ends with the specified string. • `equals` - Matches only if the header name completely matches the specified string • `starts-with` - Matches only if the header name starts with the specified string. The value in this command is not case-sensitive.
[no] header-value *match-option string* {**service-group** service-*group-name*}	Matches based on the value of the header. Descriptions of the match-options are mentioned below: • `contains` - Matches if the specified string appears anywhere within the header value. • `ends-with` - Matches only if the header value ends with the specified string. • `equals` - Matches only if the header value completely matches the specified string • `starts-with` - Matches only if the header value starts with the specified string. The value in this command is not case-sensitive.
[**no**] **host** *match-option URL-string* {**service-group** *service-group-name}*	Matches based on host names. Descriptions of the match-options are mentioned below: • `contains` - Matches if the specified string appears anywhere within the host name. • `ends-with` - Matches only if the host name ends with the specified string.

Command	Description
	• `equals` - Matches only if the host name completely matches the specified string. • `starts-with` - Matches only if the host name starts with the specified string. The value in this command is not case-sensitive.
multi-match-rule *rule-name sequence-number* *{option}*	Matches the rules based on the multiple conditions. Descriptions of the parameters are given below: • *`rule-name`*: Specifies the name of the rule. • *`sequence-number`*: Specifies the unique number between 1-8192. The multi-match-rule objects are matched according to this sequence number. For example, if the incoming HTTP request satisfies two rules, the rule with the smaller sequence number is selected. This command enters the multi-match-rule Configuration mode where the following *options* are available. • `cookie-name` - Specifies the cookie-name to be matched. • `cookie-value` - Specifies the cookie-value to be matched. • `cookie-name-value-match` - Matches requests only if the exact cookie name and value pair are present. This setting can only be configured when both **`cookie-name`** and **`cookie-value`** rules are defined. • `header-name` - Specifies the header-name to be matched.

Command	Description
	• `header-value` - Specifies the header value to be matched. • `header-name-value-match` - Matches requests only if the exact header name and value pair are present. This setting can only be configured when both **`header-name`** and **`header-value`** rules are defined. • `host` - Specifies the host name to be matched. • `url` - Specifies the URL to be matched. • The selection of the service group is made based on the **`sequence-number`**r; smaller **`sequence-number`** has the highest priority. We do not select the service group unless **all** the options are satisfied. **NOTE:** • The maximum number of rules supported are 1023. • In case of multi-match-rule objects, for each parameter value, there can only be one condition. For example, **`host contains a`** and **`host contains b`** cannot co-exist under the same template. • Single-match-rules and multi-match-rules are mutually exclusive; they cannot be used together. • The condition type **`geo-location`** is not supported for the **`multi-match-rule`**.
	Matches based on query name. Descriptions of the match-options are mentioned below:

Command	Description
[no] query-param-name *match-option string* {**service-group** *service-group-name*}	• `contains` - Matches if the specified string appears anywhere within the query name. • `ends-with` - Matches only if the query name ends with the specified string. • `equals` - Matches only if the query name completely matches the specified string. `query-param-name equals` [*no-name*] is considered as a condition that matches a query with an empty name. • `starts-with` - Matches only if the query name starts with the specified string. The value in this command is case-sensitive.
[no] query-param-value *match-option string* {**service-group** *service-group-name*}	Matches based on query value. Descriptions of the match-options are mentioned below: • `contains` - Matches if the specified string appears anywhere within the query value. • `ends-with` - Matches only if the query value ends with the specified string. • `equals` - Matches only if the query value completely matches the specified string. `query-param-value equals` [*no-value*] is considered as a condition that matches a query with an empty value. • `starts-with` - Matches only if the query value starts with the specified string. The value in this command is case-sensitive.
[**no**] **url** *match-option url-string* {**service-group**	Matches based on URL strings. Descriptions of the match-options are mentioned below: • `contains` - Matches if the specified string appears anywhere within the URL.

Command	Description
`service-group-name}`	• `ends-with` - Matches only if the URL ends with the specified string. • `equals` - Matches only if the URL completely matches the specified string. • `starts-with` - Matches only if the URL starts with the specified string. The value in this command is case-sensitive. **NOTE:** This condition type does not support query strings. For example, if you set the condition as **`url contain/index.html?name=abc`**,the request **`http://<domain>/index.html?name=abc`** will not match. However, if you set the condition as **`url contains /index.html`**, the request will match.

Usage

These match options are always applied in the order shown above, regardless of the order in which the rules appear in the configuration.

If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a URL matches on more than one of them, the most-specific match is always used.

A template can have a single-match rule or multi-match rules. The **`multi-match-rule`** is used when multiple rules need to be specified. The **`multi-match-rule`** objects are matched according to the given sequence number. For example, if the incoming HTTP request satisfies two rules, the rule with the smaller sequence number is selected.

The configuration of the multi-match-rule is case sensitive. The case-sensitive parameters must be used in the appropriate case for the desired functioning of the multi-match-rule. The case-insensitive parameters are normalized to lower-case and accordingly used in matching. This behavior is applicable for HTTP 1.1 and HTTP/2 protocols.

NOTE: Different rules specified under the single-match-rule use the **OR** relationship. However, multiple rules specified under the **multi-match-rule** use the **AND** relationship.

NOTE: A **query-param-name** and **query-param-value**condition match works only if the query string is included in the url and not in the request body. Additionally, match with these condition types does not decode url-encoding. Therefore, to match a space (" "), you need to specify "%20".

Example The following example demonstrates single-match-rule usage :

```
ACOS(config)#slb template http-policy http-policy4.2.6
ACOS(config-http-policy)#header-name contains A service-group
http-policy-sg-A
```

Example The following example demonstrates **multi-match-rule** usage:

```
ACOS(config)#slb template http-policy http-policy4.2.6
ACOS(config-http-policy)# multi-match-rule A 1024
ACOS(config-http-policy-multi-match-rule)# host contains A1
ACOS(config-http-policy-multi-match-rule)# url contains
exdomain
ACOS(config-http-policy-multi-match-rule)# cookie-name
contains _Sec
ACOS(config-http-policy-multi-match-rule)# service-group http-
policy-sg-A
```

Example The following example demonstrates **query-param-name** condition type usage:

```
ACOS(config)#slb template http-policy http-policy4.2.6
ACOS(config-http-policy)# query-param-name contains fname
service-group http-policy-sg-A
ACOS(config-http-policy)# query-param-name equals [no-name]
service-group http-policy-sg-B
```

Example The following example demonstrates **query-param-value** condition type usage:

```
ACOS(config)#slb template http-policy http-policy4.2.6
```

```
ACOS(config-http-policy)# query-param-value ends-with fname
service-group http-policy-sg-A
ACOS(config-http-policy)# query-param-value equals [no-value]
service-group http-policy-sg-B
```

Example The following example demonstrates multi-match-rule usage with cookie-name-value-match and header-name-value-match settings:

```
ACOS(config)#slb template http-policy h1
ACOS(config-http-policy)# multi-match-rule A 1024
ACOS(config-http-policy-multi-match-rule)# host contains A1
ACOS(config-http-policy-multi-match-rule)# url contains
exdomain
ACOS(config-http-policy-multi-match-rule)# cookie-name
contains _Sec
ACOS(config-http-policy-multi-match-rule)# service-group http-
policy-sg-A
ACOS(config-http-policy-multi-match-rule)# cookie-value
contains SecretValue
ACOS(config-http-policy-multi-match-rule)# cookie-name-value-
match
ACOS(config-http-policy-multi-match-rule)# header-name
contains X-Custom-Header
ACOS(config-http-policy-multi-match-rule)# header-value
contains HeaderValue
ACOS(config-http-policy-multi-match-rule)# header-name-value-
match
ACOS(config-http-policy-multi-match-rule)# service-group http-
policy-sg-A
```

slb template imap-pop3

Description Configure an IMAP/POP3 template.

Syntax

```
[no] slb template imap-pop3 template-name
```

Replace **template-name** with the name of the template, up to 31 characters long.

This command enters the SLB IMAP Template Configuration mode where the following commands are available:

Command	Description
logindisabled	When used, the server will expect the login to be in an encrypted format. This option is only valid for IMAP configuration.
starttls {**disabled** | **optional** | **enforced**}	Configure whether or not STARTTLS is used. • **disabled** - the ACOS device will not support STARTTLS. • **optional** - the ACOS device will not expect STARTLS and can function without using SSL. • **enforced** - for IMAP., only the CAPABILITY command can precede STARTTLS; all other commands are rejected. For POP3, no commands are allowed before STARTTLS; all commands are rejected.

Default The configuration does not have a default logging template.

Mode Configuration mode

Example The following example configures an IMAP template with STARTTLS enforced, then applies the template to a virtual port:

```
ACOS(config)# slb template imap-pop3 imap-temp
ACOS(config-imap-pop3)# logindisabled
ACOS(config-imap-pop3)# starttls enforced
ACOS(config-imap-pop3)# exit
ACOS(config)# slb virtual-server imap-vserver
ACOS(config-slb vserver)# port 143 imap
ACOS(config-slb vserver-vport)# template imap-pop3 imap-temp
```

slb template link-block-as-down

Description Enable the link-down template for LACP Link-block.

Syntax `[no] slb template link-block-as down enable`

Default Disabled.

Mode Configuration mode

Usage .

Example The following example enables a link-down template:

```
ACOS(config)# slb template link-block-as down enable
```

slb template link-cost

Description Configure the link-cost template.

Syntax `[no] slb template link-cost template-name`

Replace **template-name** with the name of the template, up to 31 characters long.

This command enters the SLB link-cost Template Configuration mode where the following commands are available:

Command	Description
bandwidth-interval *interval*	Specify the interval for bandwidth accounting. The interval can be from 1 to 60 seconds. The default is 5 seconds.
overage-bandwidth-cost *number*	Specify the overage bandwidth cost per interval. The value can be from 0 to 4294967295. The default is 0.
prepaid-bandwidth *number*	Specify the prepaid bandwidth per interval. The value can be from 0 to 4294967295. The default is 0.
sampling-enable	Enable sampling to display the statistics. The following parameters can be selected:

Command	Description
	• **all**: Display all the parameters (mentioned below) • **link_total_fwd_bytes**: Total number of bytes forwarded for a link • **interval_fwd_bytes**: Total number of bytes transferred in the forward direction per interval • **link_total_conn**: Total link cost for the connection • **interval_avg_throughput**: Average throughput per interval • **interval_max_throughput**: Maximum throughput per interval

Default The configuration has a default logging template.

Mode Configuration mode

Usage This template can be configured under an **slb server** object.

NOTE: The average throughput and maximum throughput is calculated based on interval set during configuration and may not match ISP calculations. Additionally, the cost estimated based on interval provided may not reflect which ISP is used to calculate the cost.

Example The following example configures a link-cost template:

```
ACOS(config)# slb template link-cost ln1
ACOS(config-rserver)# bandwidth-interval 10
ACOS(config-rserver)# prepaid-bandwidth 10
ACOS(config-rserver)# overage-bandwidth 5
```

slb template link-down-on-restart

Description Enable the link-down template for all the LACP link event.

Syntax `[no] slb template link-down-on-restart enable`

Default Disabled.

Mode Configuration mode

Usage .

Example The following example enables link-down template:

```
ACOS(config)# slb template link-down-on-restart enable
```

slb template link-probe

Description Configure a global command with link-probe settings.

Syntax `[no] slb template link-probe <template-name>`

Parameter	Description
slb template link-probe	Creates a template that can be applied under a service-group when method "next-hop-link" is configured.
template-name	Specify the name of the template, up to 127 characters long.

Default The configuration does not have a default link-probe template.

Mode Global Configuration mode

Usage This command enters the SLB Template Configuration mode where additional commands are available.

Example To configure an SLB template:

```
ACOS(config)#slb template link-probe IpTemplate
ACOS(config-probe template)#?
```

destination hostname

Description Configure a destination hostname for link probe template.

Syntax

```
destination hostname <host_name> {resolve-to-ipv4 | resolve-
to-ipv6 | static-ipv4-addr | static-ipv6-addr}
```

Parameter	Description
host_name	Replace host-name with the name of the template, 1 to 127 target characters long.

Mode Link-probe template mode

Example The following example configures a slb template link-probe with destination hostname and static/dynamic ip address (ipv4/ipv6). Only one hostname+ip combination is allowed inside a template:

```
ACOS(config-probe template)# destination hostname www.probe-
template-dest.com resolve-to-ipv4
ACOS(config-probe template)# destination hostname www.probe-
template-dest.com resolve-to-ipv6
ACOS(config-probe template)# destination hostname www.probe-
template-dest.com
static-ipv4-addr 172.16.213.94
ACOS(config-probe template)# destination hostname www.probe-
template-dest.com
static-ipv6-addr 172::94
```

destination hostname target

Description Configure destination hostname with static or DNS resolution type

Syntax

```
destination hostname <host_name>
 {resolve-to-ipv4 | resolve-to-ipv6 |
 static-ipv4-addr | static-ipv6-addr}
```

Command	Description
`destination hostname <host_name>`	Configure destination hostname with static or DNS resolution type. Replace `host-name` with the name of the template, 1 to 127 characters long.
`resolve-to-ipv4`	Use a query only to resolve the configured

Command	Description
	hostname.
`resolve-to-ipv6`	Use AAAA query only to resolve the configured hostname.
`static-ipv4-addr`	Target IPv4 address.
`static-ipv6-addr`	Target IPv6 address.

Example The following example configures a slb template link-probe with destination hostname and static/dynamic ip address (IPv4 or IPv6). Only one hostname +IP combination is allowed inside a template:

```
ACOS(config-probe template)# destination hostname
www.probe-template-dest.com resolve-to-ipv4
ACOS(config-probe template)# destination hostname
www.probe-template-dest.com resolve-to-ipv6
ACOS(config-probe template)# destination hostname
www.probe-template-dest.com static-ipv4-addr 172.16.213.94
ACOS(config-probe template)# destination hostname
www.probe-template-dest.com static-ipv6-addr 172::94
```

expected-status-code

Description Configure an expected-status-code.

Syntax

```
[no] expected-status-code <value>
```

Parameter	Description
value	Name of the template 1 to 31 characters long. The format is xx, xx-xx.

Default Default value is 200.

Mode Link probe template mode.

Example This is the code that is delivered when a web page or resource acts exactly the way it's expected to load.

Success codes returned when browser request was successfully received, understood, and processed by the server.

The following example configures the expected status-codes to look for in a probe http connection in order to record RTT measurement:

```
ACOS(config-probe template)# expected-status-code 200, 201-
299,
301-302
ACOS(config-probe template)# expected-status-code 200, 201
ACOS(config-probe template)# expected-status-code 301
```

probe-interval

Description Configure a probe-interval for the link probe.

Syntax

```
[no] probe-interval <time_in_seconds>
```

Parameter	Description
probe-interval <*time_in_seconds*>	Configure probe-interval, that is the time between two successive probes. Replace seconds with the values in seconds 1 to 2147483647. The default is 5 seconds.

Default Default interval is 5 seconds.

Mode Link Probe Template mode.

Example The following example configures the probe-interval:

```
ACOS(config-probe template)# probe-interval 5
```

probes-per-test

Description Configure number of probes-per-test.

Syntax

```
[no] probes-per-test <number>
```

Parameter	Description
probes-per-test <*int-probes-per-test*>	Total number of probes that need to be sent out for each test. The test value is 1 to 10.

Default The default is 5.

Mode Link probe template mode

Example The following example configures the `probes-per-test` parameter.

```
ACOS(config-probe template)# probes-per-test 3
```

rtt-method

Description Configure a rtt-method type for link probe.

Syntax

```
[no] rtt-method {http rtt | tcp rtt}
```

Parameter	Description
http rtt	Calculate Round Trip Time between HTTP request and response.
tcp rtt	Use the TCP Smoothed round trip time in the HTTP connection. TCP SRTT is calculated for the TCP connection up to the point of receiving an expected HTTP response.

Default This is the default rtt-method.

Mode Link probe template mode.

Usage Round-trip time (RTT) is the duration in milliseconds it takes for a network request to go from a starting point to a destination and back again to the starting point.
RTT sample will be marked as error, if an unexpected HTTP status code or TCP status is received or a network error occurs.

Example Calculate Round Trip Time between HTTP request and response. RTT sample will be marked as error, if an unexpected HTTP status code is received or a network error occurs.

The following example configures the rtt-method to be used inside the link-probe template:

```
ACOS(config-probe template)# rtt-method http-rtt
ACOS(config-probe template)# rtt-method tcp-srtt
```

selection-rule

Description Specify the link selection strategy for link-probe template.

Syntax

```
[no] selection-rule {fastest-link-always | threshold}
```

Parameter	Description
fastest-link-always	Specify the option to always use the link with the lowest average latency.
threshold	Specify the option to use all links below a threshold before selecting the fastest link. Numerical value within a range of 1-65534 should be specified for the threshold parameter. For example, *selection-rule threshold 10*.

Default If *selection-rule* is not specified, the default parameter is the *fastest-link-always*.

Mode Link probe template mode.

Example The following examples configure the selection-rule:

```
ACOS(config-probe template)# selection-rule fastest-link-
always
ACOS(config-probe template)# selection-rule threshold 10
```

test-interval

Description Configure a test-interval for link-probe template.

Syntax

```
[no] test-interval <test_interval>
```

Parameter	Description
<test_interval>	The time interval between subsequent tests, the values in seconds 1 to 2147483647. It is the time interval between subsequent tests. Configuring a larger test-interval then the probe-interval will result in a more stable link selection.

Default The default is 60 seconds.

Mode Link probe template mode.

Example The following example configures the test-interval:

```
ACOS(config-probe template)# test-interval 60
```

url

Description Configure an URL for link probe. Specify URL to which probes should be sent out.

Syntax

```
[no] url <name>
```

Parameter	Description
name	Replace name with the name of the template 1 to1023 characters long.

Default Default is /

Mode Link probe template mode.

Example The following example configures the url:

```
ACOS(config-probe template)# url www.123xyz.com
```

user-tag

Description Configure a user-tag and associate it to link probe template.

Syntax

```
[no] user-tag <name>
```

Parameter	Description
user-tag <*name*>	Name of the template 1 to 127 characters long. The character length is 1 to 127.

Default The default is 60 seconds.

Mode Link probe template mode.

Usage This is very useful method of creating and managing website or module permissions. You can customize the tags to the users.

Example The following example configures a user-tag:

```
ACOS(config-probe template)# user-tag 1
```

slb template logging

Description Configure external logging over TCP.

Syntax

```
[no] slb template logging template-name
```

Replace **template-name** with the name of the template, up to 31 characters long.

NOTE: The minimum and maximum configurable values are platform specific. To check the configurable values, use the **show slb resource-usage** command.

This command enters the SLB Logging Template Configuration mode where the following commands are available.

Command	Description
[**no**] **format** *string*	Configures a log string. Web logging is described in detail in the “Web Logging for HTTP and RAM Caching” section of the *Application Delivery Controller Guide*.
[**no**] **local-**	Enables or disables local logging:

Command	Description
logging {0 | 1}	• 0 – Disables local logging. • 1 – Enables local logging. The default is 0 (disabled).
[**no**] **pcre-mask** *pattern* [**keep-end** *num* | **keep-start** *num* | **mask** *char*]	Mask matched Perl Compatible Regular Expression (PCRE) pattern in the log. • Use **keep-end** to specify the number of unmasked characters to keep at the end (0-65535); the default is 0. • Use **keep-start** to specify the number of unmasked characters to keep at the start (0-65535); the default is 0. • Use **mask** to specify a character to use as the mask for the matched pattern; the default is "X".
[**no**] **service-group** *group-name*	For remote logging, specifies the name of the service group that contains the log servers.
[**no**] **template tcp-proxy** *template-name*	Binds a TCP-proxy template to the logging template.

Default The configuration does not have a default logging template.

Mode Configuration mode

Usage Logging over TCP also requires some additional configuration. For more information, see*Application Delivery Controller Guide*.

slb template mqtt

Description Configures a template for MQTT load balancing.

Syntax

```
[no] slb template mqtt template-name
```

Replace template-name with a name, up to 127 characters. This command enters the template configuration mode where the following commands are available.

Command	Description
[no] cli-entid-hash-persist {**First** | **Last** | **Off-set**} *number*	Use client identifier (client ID) of the MQTT CONNECT message to assign a hash value for selecting an MQTT broker server. The following hash options are available. • **first & last** — Specifies which end of the client id string to use for calculating the hash value. The number indicates the number of characters in the client ID, counted from the first or the last character of the ID. The number must be in the range of 4–128. • **offset** — Specifies how far into the string to begin hash calculation. The number indicates the skipped characters in the client ID. The number must be in the range of 0–255.

Default N/A

Mode Configuration Mode

Usage All MQTT packet flow occurs between the MQTT client and the MQTT broker. The client Id identifies each MQTT client that connects to an MQTT broker.

ACOS uses hash-based load balancing to select an MQTT broker server based on the client ID and maintain a persistent connection. The ACOS device receives the MQTT message from the client, parses it, and load balances to the broker server (forwards the MQTT packet).

Example The following commands configure an MQTT template named ‘mq-1’. In this MQTT template, server selection will be based on the client ID-

based hash value, and the last 4 characters of the client ID will be used to achieve hash-based persistence.

```
ACOS(config)# slb template mqtt mq-1
ACOS(config-mqtt)# clientid-hash-persist last 4
ACOS(config-mqtt)# exit
```

The following commands binds the MQTT template named 'mq-1' to the virtual server.

```
ACOS(config)# slb virtual-server vs1 10.1.1.1
ACOS(config-slb vserver)# port 1883 mqtt
ACOS(config-slb vserver-vport)# template mqtt mq-1
```

slb template monitor

Description Configure a link monitoring template.

Syntax

```
[no] slb template monitor num
```

Replace *num* with the identification number of the template. This can be a number between 1 to 16.

This command enters the SLB Monitor Template Configuration mode where the following commands are available.

Command	Description
[no] **action** *options*	Specifies the action to perform when a monitored event is detected. • **clear sessions** {**all** | **sequence** *portnum*} • **link-disable eth** *portnum* **sequence** *portnum* • **link-enable eth** *portnum* **sequence** *portnum*
[no] **monitor** *options*	Specifies the events and links (Ethernet data ports) to monitor. The sequence number assigned to monitoring entries specify the order in which to check the monitored ports for the specified event type. • **link-down eth** *portnum* [**eth** *portnum* ...]

Command	Description
	sequence *order* • **link-up eth** *portnum* [**eth** *portnum* ...] **sequence** *order*
[**no**] **monitor-and**	Uses the logical operator "AND" for link monitoring. The actions are performed only if *all* of the monitored events are detected. This is selected by default.
[**no**] **monitor-or**	Uses the logical operator "OR". The actions are performed if *any* of the monitored events are detected.

Default The ports within a given monitor entry are always ANDed. If you specify more than one port (eth portnum option) in the same monitor entry, the specified event must occur on all the ports in the entry. For example, if you specify link-down eth 9 eth 11, the link must go down on ports 9 and 11, for the link-state changes to count as a monitored event.

Mode Configuration mode

Usage The logical operator applies only to monitor entries, not to action entries. For example, if the logical operator is OR, and at least one of the monitored events occurs, all the actions configured in the template are applied.

You can configure the entries in any order. In the configuration, the entries of each type are ordered based on sequence number.

Example The following commands configure monitor template 1:

```
ACOS(config)# slb template monitor 1
ACOS(config-monitor)# monitor-or
ACOS(config-monitor)# monitor link-down eth 5 sequence 1
ACOS(config-monitor)# monitor link-down eth 6 sequence 2
ACOS(config-monitor)# monitor link-down eth 9 sequence 3
ACOS(config-monitor)# monitor link-down eth 10 sequence 4
ACOS(config-monitor)# action clear sessions sequence 1
ACOS(config-monitor)# action link-disable eth 5 sequence 2
ACOS(config-monitor)# action link-disable eth 6 sequence 3
```

```
ACOS(config-monitor)# action link-disable eth 9 sequence 4
ACOS(config-monitor)# action link-disable eth 10 sequence 5
```

Example The following example shows how to use the SLB link monitoring command in a CGN shared partition:

```
ACOS(config)# allow-slb-cfg enable
ACOS(config)# slb template monitor 1
ACOS(config-monitor)# monitor-or
ACOS(config-monitor)#
```

slb template persist cookie

Description Configure session persistence by inserting persistence cookies into server replies to clients.

Syntax

```
[no] slb template persist cookie template-name
```

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters the SLB Persist Cookie Template Configuration mode where the following commands are available.

Command	Description
[no] domain *domain-name*	Adds the specified domain name to the cookie.
[no] dont-honor-conn-rules	Ignores connection limit settings configured on real servers and real ports. This option is useful for applications in which multiple sessions (connections) are likely to be used for the same persistent cookie. By default, this is disabled; the connection limit set on real servers and real ports is used.
[no] encrypt-level *0* | *1*	Sets the encryption level for cookie name or value. The encryption level can be set to 0 or 1. • 0 – Indicates plain text.

Command	Description
	• 1 – Indicates that the text is encrypted. This is the default option. **NOTE:** Cookie encryption applies only for those cookies generated by ACOS.
`[no] expire` *seconds* **use-attributes** *options*	Specifies the expiration time, in seconds, after which the cookie is deleted from the client's browser. The default value is 1 year (31,536,000 seconds). The **use-attributes** command lets you choose the attributes that ACOS should insert into the cookie: • `max-age` – ACOS inserts the max-age attribute , which sets the expiry time, in seconds, for the cookie. The cookie expires from the client's PC after the defined number of seconds. For example, if the **expire** value is set to 120 seconds and the max-age attribute is used, the cookie will expire 120 seconds after it is received on the client side. The max-age is independent of the date and time configuration between ACOS and the client. This attribute is useful to avoid cookie expiration in case the clocks on the client and the ACOS are not in sync. • `expires` – ACOS uses the expires attribute to set an expiry date and time. The cookie expires at the date and time mentioned. For example, if the **expire** value is set to 120 seconds, and if the client is configured with 10 minutes advance time as compared to ACOS, then the cookie will expire immediately once the client-side receives it due to date and time setting.

Command	Description
	• `all` – ACOS inserts both, the `max-age` and `expires` attributes. If this is set, the `max-age` attribute takes precedence and controls the cookie expiration for clients who implement this feature.
[**no**] **httpOnly**	Sets the HTTP-only flag in the persistence cookie.
[**no**] **insert-always**	Specifies whether to insert a new persistence cookie in every reply, even if the request already had a persistence cookie previously inserted by the ACOS device. This is disabled by default; the ACOS device inserts a persistence cookie only if the client request does not already contain a persistence cookie inserted by the ACOS device, or if the server referenced by the cookie is unavailable.
[**no**] **match-type** {**server** [**service-group**] | **service-group**} [**scan-all-members**]	Changes the granularity of cookie persistence. • **server** – The cookie inserted into the HTTP header of the server reply to a client ensures that subsequent requests from the client for the same VIP are sent to the same real server. (This assumes that all virtual ports of the VIP use the same cookie persistence template with match-type set to **server**.) Without this option, the default behavior is used: subsequent requests from the client will be sent *to the same real port* on the same real server. • **server service-group** – Sets the granularity to the same as **server**, and also enables cookie persistence to be used along with URL switching or host switching. Without the **service-group** option, URL switching or host switching can be used only for the initial request from the client.

Command	Description
	After the initial request, subsequent requests are always sent to the same service group. • **service-group** – This option enables support for URL switching and host switching, along with the default cookie persistence behavior. • **scan-all-members** – This option scans all members bound to the template. This option is useful in configurations where match-type "server" is used, *and* where some members have different priorities or are disabled. (For more information about this option, see the "Scan-All-Members Option in Persistence Templates" chapter in the *Application Delivery Controller Guide*.) **NOTE:** To use URL switching or host switching, you also must configure an HTTP template with the **host-switching** or **url-switching** command. The default match type is **port**. (There is no **port** keyword. See "Usage" for more information.)
[**no**] **name** *cookie-name*	Specifies the name of the persistence cookie, 1-63 characters. The default name is "sto-id".
[**no**] **pass-thru**	Enables pass-through mode for passive cookie persistence. This is disabled by default.
[**no**] **pass-phrase** *pass-word*	Sets the encryption level for cookie name value pair generated by ACOS. Sets the password for encryption when the option **encrypt-level** is set to 1. The password should be of 8 characters. Failure to remember the password may create a problem while trying to unset the password as the

Command	Description
	password is not visible as plain text. If the password cannot be retrieved, set a new password to overwrite the existing password. **NOTE:** The following special characters are supported for the password: ~!@#$%^&*()-_+=,.<>/;:
[**no**] **path** *path-name*	Adds path information to the cookie, 1-31 characters. The default path is "/".
[**no**] **samesite** {**none** | **lax** | **strict**}	Set cookie same-site attribute. • **none** – The cookie was sent in all contexts. • **lax** – The cookie was sent on same-site requests and on cross-site requests. • **strict** – The cookie was sent only in same-site contexts.
[**no**] **secure**	Enables secure attribute.

Default The configuration does not have a default cookie-persistence template. If you create one, it has the defaults described in the table above.

Mode Configuration mode

Usage The normal form of this command creates a cookie-persistence template. The **no** form of this command removes the template.

You can bind only one cookie-persistence template to a virtual port. However, you can bind the same cookie-persistence template to multiple ports.

When cookie persistence is configured, the ACOS device adds a persistence cookie to the server reply before sending the reply to the client. The client's browser re-inserts the cookie into each request.

For security, address information in the cookie is encrypted.

The format of the cookie depends on the match-type setting:

- **match-type (port)** – This is the default setting. Subsequent requests from the client will be sent to the same real port on the same real server. URL switching or host switching can be used only for the first request.

  The cookie that the ACOS device inserts into the server reply has this format:

  ```
  Set-Cookie: cookiename-vport=rserverIP_rport
  ```

  The *vport* is the virtual port number. The *rserverIP* is the real server IP address and the *rport* is the real server port number.

  The **port** option is shown in parentheses because the CLI does not have a "port" keyword. If you do not set the match type to **server** (see below), the match type is automatically "port".

- **match-type server** – Subsequent requests from the client for the same VIP will be sent to the same real server, provided that all virtual ports of the VIP use the same cookie persistence template with match-type set to server. URL switching or host switching can be used only for the first request.

  The cookie that the ACOS device inserts into the server reply has this format:

  ```
  Set-Cookie: cookiename=rserverIP
  ```

- **match-type (port) service-group** – Subsequent requests from the client will be sent to the same real port on the same real server, within the service group selected by URL switching or host switching. URL switching or host switching, if configured, is still used for every request.

  The cookie that the ACOS device inserts into the server reply has the following format:

  ```
  Set-Cookie: cookiename-vport-
  servicegroupname=rserverIP_rport
  ```

- **match-type server service-group** – Subsequent requests from the client for the same VIP will be sent to the same real server, within the service group selected by URL switching or host

switching. URL switching or host switching, if configured, is still used for every request.

The cookie that the ACOS device inserts into the server reply has the following format:

```
Set-Cookie: cookiename-servicegroupname=rserverIP
```

Example The following commands configure a cookie persistence template named “persist-cookie”. The template inserts a cookie named “MyCookie”, containing the real server’s IP address and protocol port in encrypted form, into server responses before sending the responses to clients. The template also sets the cookie to persist on client PCs for only 10 minutes (600 seconds).

```
ACOS(config)# slb template persist cookie persist-cookie
ACOS(config-cookie persist)# name MyCookie
ACOS(config-cookie persist)# expire 600
```

Example The following command configures the passphrase. Also, the example includes the command to unset the passphrase and the message displayed if incorrect password is entered while trying to unset the password.

```
ACOS(config-cookie persist)# passphrase abcd1234
ACOS(config-cookie persist)# no passphrase aaaaaaaa
Field value does not match (field: aaaaaaaa)
ACOS(config-cookie persist)#no passphrase abcd1234
ACOS(config-cookie persist)#
```

slb template persist destination-ip

Description Configure the granularity of load balancing persistence (selection of the same server resources) for clients, based on destination IP address.

Syntax

```
[no] slb template persist destination-ip template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB Persist Destination-IP Template Configuration mode where the following commands are available.

Command	Description
[no] dont-honor-conn-rules	Ignores connection limit settings configured on real servers and real ports. This option is useful for applications in which multiple sessions (connections) are likely to be used for the same persistent destination IP address. This is disabled by default; the connection limit set on real servers and real ports is used.
[no] hash-persist	Enables hash-based persistence. Hash-based persistence provides the persistence and performance benefits of hash-based load balancing, while allowing use of advanced SLB features that require stateful load balancing. For more information, see "Hash-based IP Persistence" in the *Application Delivery Controller Guide*.) This is disabled by default.
[no] match-type {server | service-group} [scan-all-members]	Specifies the granularity of persistence: • server – Traffic to a given destination IP address is always sent to the same real server, for any service port. By default (without the **server** option), traffic to the same destination IP address and virtual port is always sent to the same real port. This is the most granular setting. • service-group – This option is applicable if you also plan to use URL switching or host switching. If you use the **service-group** option, URL or host switching is used for every request to select a service group. The first time URL or host switching selects a given service group, the load-balancing method is used to select a real port within the service group. The next time URL or host switching selects the same service

Command	Description
	group, the same real port is used. Thus, service group selection is performed for every request, but once a service group is selected for a request, the request goes to the same real port that was selected the first time that service group was selected. • `scan-all-members` – This option scans all members bound to the template. This option is useful in configurations where match-type "server" is used, *and* where some members have different priorities or are disabled. (For more information about this option, see the "Scan-All-Members Option in Persistence Templates" chapter in the *Application Delivery Controller Guide*.) To use URL switching or host switching, you also must configure an HTTP template with the **`host-switching`** or **`url-switching`** command. For SLB, by default, traffic to a given destination IP address and port is always sent to the same real port. This is the most granular setting. (There is no **`port`** keyword.)
[**no**] **`netmask`** *`ipaddr`*	Specifies the granularity of IPv4 address hashing for initial server port selection. You can specify an IPv4 network mask in dotted decimal notation. • To configure initial server port selection to occur once per destination VIP subnet, configure the network mask to indicate the subnet length. For example, to select a server port once for all requested VIPs within a subnet such as 10.10.10.x, 192.168.1.x, and so on ("class C" subnets), use mask 255.255.255.0. SLB selects a server port for the first request to the given VIP subnet, the sends all other

Command	Description
	requests for the same VIP subnet to the same port. • To configure initial server port selection to occur independently for each requested VIP, use mask 255.255.255.255. (This is the default.)
[**no**] **netmask6** *mask-length*	Specifies the granularity of IPv6 address hashing for initial server port selection. (See above for more information.), The default is 128.
[**no**] **timeout** *timeout-minutes*	Specifies how many minutes the mapping remains persistent after the last time it is used. You can specify 1-2000 minutes. The default is 5 minutes.

Default The configuration does not have a default destination-IP persistence template. If you configure one, it has the defaults specified in the table above.

Mode Configuration mode

Usage The normal form of this command creates a destination-IP persistence template. The "**no**" form of this command removes the template.

You can bind only one destination-IP persistence template to a virtual port. You can bind the a destination-IP persistence template to multiple ports.

Use of the service-group match-type option **scan-all-members** is not useful in conjunction with destination-IP persistence templates, and is not supported.

Example The following command creates a destination-IP persistence template named "persist-dest":

```
ACOS(config)# slb template persist destination-ip persist-source
```

slb template persist source-ip

Description Configure the granularity of load balancing persistence (selection of the same server resources) for clients, based on source IP address.

Syntax

```
[no] slb template persist source-ip template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB Persist Source-IP Template Configuration mode, where the following commands are available.

Command	Description
[no] dont-honor-conn-rules	Ignores connection limit settings configured on real servers and real ports. This option is useful for applications where multiple sessions (connections) will likely to be used for the same persistent client source IP address. This is disabled by default; the connection limit set on real servers and ports is used.
[no] enforce-higher-priority	Enables Source-IP Persistence Override and Reselect. When this feature is enabled, the ACOS device continually checks for higher-priority servers, even if source-IP persistence is enabled and sessions are already established between client and server.
[no] hash-persist	Enables hash-based persistence. Hash-based persistence provides the persistence and performance benefits of hash-based load balancing, while allowing advanced SLB features that require stateful load balancing. This is disabled by default.
[no] incl-dst-ip	Used to support the ALG protocol firewall load balancing feature for protocols such as FTP. This option helps ensure that a special persistent session will be matched on both the source IP and destination

Command	Description
	IP addresses.
[no] **incl-sport**	Includes the source port in persistent sessions. This is disabled by default.
[no] **match-type** {**server** [**scan-all-members**] | **service-group**}	Specifies the granularity of persistence: • **server** – Traffic from a given client to the same VIP is always sent to the same real server for any service port requested by the client. By default (without the **server** option), traffic from a given client to the same virtual port is always sent to the same real port. This is the most granular setting. ◦ The **scan-all-members** option scans all members bound to the template. This option is useful in configurations where match-type "server" is used *and* where some members have different priorities or are disabled. • **service-group** – This option is applicable if you also plan to use URL switching or host switching. If you use the **service-group** option, URL or host switching is used for every request to select a service group. The first time URL or host switching selects a given service group, the load-balancing method is used to select a real port within the service group. The next time URL or host switching selects the same service group, the same real port is used. Thus, service group selection is performed for every request, but once a service group is selected for a request, the request goes to the same real port that was selected the first time that service group was selected.

Command	Description
	To use URL switching or host switching, you also must configure an HTTP template with the **host-switching** or **url-switching** command. **NOTE:** The match type for FWLB is always **server**, which sets the granularity of source-IP persistence to individual firewalls, not firewall groups or individual service ports. • For SLB, by default, traffic from a given client to the same virtual port is always sent to the same real port. This is the most granular setting. (There is no **port** keyword.) • For FWLB, the default is **server**, and none of the other **match-type** options are applicable.
[**no**] **netmask** *ipaddr*	Specifies the granularity of IP address hashing for server port selection. • To configure server port selection to occur per subnet basis, configure the network mask to indicate the subnet length. For example, to send all clients within a subnet such as 10.10.10.x, 192.168.1.x, and so on ("class C" subnets) to the same server port, use mask 255.255.255.0. SLB selects a server port for the first client in a given subnet, the sends all other clients in the same subnet to the same port. • To configure server port selection to occur per client basis, use mask 255.255.255.255. SLB selects a server port for the first request from a given client, the sends all other requests from the same client to the same port. (This is the default.) The default is 255.255.255.255.
[**no**]	Specifies the granularity of IPv6 address hashing for

Command	Description
netmask6 *mask-length*	initial server port selection. (See above for more information.) The default is 128.
[**no**] **timeout** *minutes*	Specifies the persistence timeout value the mapping remains persistent after the last time traffic from the client is sent to the server. You can specify 1-4321 minutes (about 72 hours). The default timeout is 5 minutes.

Default The configuration does not have a default source-IP persistence template. If you configure one, it has the defaults described in the table above.

Mode Configuration mode

Usage The normal form of this command creates a source-IP persistence template. The “no” form of this command removes the template.

You can bind only one source-IP persistence template to a virtual port. However, you can bind the same source-IP persistence template to multiple ports.

If you use the **incl-sport** option, the IP address in the Forward Source column of **show session** output is modified to include the source port. For example, “155.1.1.151:33067” is shown as “1.151.129.43”.

Using the Same VIP and Port Number for TCP and UDP Ports

When applying the source-IP persistence template to two virtual ports with the same VIP and protocol port number but different Layer 4 protocols (TCP or UDP), member lists for the ports must be identical in both TCP and UDP service groups.

For example, the following configuration works because service groups 5060-tcp and 5060-udp have the same member list although their protocols are different.

```
slb virtual-server vip2 13.0.0.100
  port 5060  sip-tcp
    service-group 5060-tcp
    template persist source-ip per-sip
  port 5060  sip
    service-group 5060-udp
    template persist source-ip per-sip
!
slb service-group 5060-tcp tcp
  member s1 5060
  member s2 5060
!
slb service-group 5060-udp udp
  member s1 5060
  member s2 5060
```

The configuration will not work if the member lists in the service groups are different. For example, the configuration will not work if the TCP group's member list is changed to either of the following:

```
slb service-group 5060-tcp tcp
  member s3 5060
  member s4 5060
```

or

```
slb service-group 5060-tcp tcp
  member s1 5061
  member s2 5061
```

Example The following commands configure a source-IP persistence template named “persist-source” and set the granularity to the server:

```
ACOS(config)# slb template persist source-ip persist-source
ACOS(config-source ip persist)# match-type server
```

Example The following commands configure a source-IP persistence template named “persist-sg” and set the granularity to service-group for enabling URL/host switching with source IP persistence:

```
ACOS(config)# slb template persist source-ip persist-sg
ACOS(config-source ip persist)# match-type service-group
```

slb template persist ssl-sid

Description Direct clients based on SSL session ID. The persistence is based on the SSL session ID, not on the client IP address.

Syntax

```
[no] slb template persist ssl-sid template-name
```

Replace *template-name* with the name of the template, 1-127 characters.

This command enters the SLB Persist SSL-SID Template Configuration mode where the following commands are available.

Command	Description
[no] dont-honor-conn-rules	Ignores connection limit settings configured on real servers and real ports. This option is useful for applications in which multiple sessions (connections) are likely to be used for the same persistent SSL session ID. Disabled by default; the connection limit set on real servers and real ports is used.
[no] timeout *minutes*	Specifies how many minutes the mapping remains persistent after the last time traffic with the SSL session ID is sent to the server. You can specify 1-250 minutes. The default is 5 minutes.

Mode Configuration mode

Default NA.

Usage SSL session-ID persistence directs all client requests for a given virtual port, and that have a given SSL session ID, to the same real server and real port. For example, with SSL session-ID persistence configured, all client requests for virtual port 443 on virtual server 1.2.3.4 that have the same SSL session ID will be directed to the same real server and port.

When multiple ssl-sid persist sessions are created by same tuple (same source IP address and same source port) exist, and data session's age

with the same source IP and same source port is updated, then the age of the ssl-sid persist sessions are also refreshed.

You can bind one SSL session-ID persistence template to a virtual port or bind the same SSL session-ID persistence template to multiple ports.

NOTE: You cannot bind SSL session-ID persistence template to HTTPS virtual port.

To view SSL session-ID persistence statistics, use the **show slb l4** command.

Example The following commands configure an SSL session-ID persistence template named "ssl-persist" and apply it to virtual port 443 on virtual server "vip1":

```
ACOS(config)# slb template persist ssl-sid ssl-persist
ACOS(config-ssl session id persist)# exit
ACOS(config)# slb virtual-server vip1 1.2.3.4
ACOS(config-slb vserver)# port 443 tcp
ACOS(config-slb vserver-vport)# service-group https-sg1
ACOS(config-slb vserver-vport)# template persist ssl-sid ssl-persist
```

slb template policy

Description Configure a template of Policy-Based SLB (PBSLB) settings.

Syntax

```
[no] slb template policy  template-name
```

Parameter	Description
template-name	Template name (1-127 characters)

Default The configuration does not have a default SIP over UDP template.

Mode Configuration mode

Usage The normal form of this command creates a PBSLB template. The **no** form of this command removes the template.

You can bind only one PBSLB template to a virtual port. However, you can bind the same PBSLB template to multiple ports.

PBSLB configuration on a virtual port can be set either using a template or by configuring the individual settings on the port. Individual PBSLB settings *and* a PBSLB template can not be configured on the same virtual port.

Apply the Policy Globally or on Individual Virtual Ports

The ACOS device also allows policy templates to be applied at the virtual-server level. However, PBSLB does not take effect if you apply the policy template at the virtual-server level. Only class lists are supported at the virtual-server level. To use PBSLB, apply the policy template globally or on individual virtual ports.

Comparing TCP and HTTP Template Application

For HTTP virtual servers:

- Connection limits are only applied at the Layer 4 TCP level.
- For Layer 7 HTTP, either configure request limits or request-rate limits.

Consider the following example, with “example-clist” class list applied to the “example-policy” template:

```
ACOS(config)# class-list example-clist
ACOS(config-class list)# 100.1.0.0/16 lid 1
ACOS(config-class list)# exit
ACOS(config)# slb template policy sample-policy
ACOS(config-policy)# class-list example-clist
ACOS(config-policy-class-list:example-cl...)# lid 1
ACOS(config-policy-class-list:example-cli...)# conn-limit 5
ACOS(config-policy-class-list:example-cli...)# over-limit-
action forward log
ACOS(config-policy-class-list:example-cli...)# exit
ACOS(config-policy-class-list:example-cl...)# exit
ACOS(config-policy)# exit
```

This template can be applied to the following virtual server at Layer 4 TCP:

```
ACOS(config)# slb virtual-server example-vs-tcp 30.1.1.100
```

```
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# template policy sample-policy
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

However, for the following virtual server, the “example-policy” template does not take effect, since connection limits are not applied at Layer 7 HTTP level:

```
ACOS(config)# slb virtual-server example-vs-http 40.1.1.100
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template policy sample-policy
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

For the “example-vs-http” virtual server, you must configure request limits and request rate limits. For example:

```
ACOS(config)# slb template policy sample-policy-2
ACOS(config-policy)# class-list example-clist
ACOS(config-policy-class-list:example-cl...)# lid 1
ACOS(config-policy-class-list:example-cli...)# request-limit
10
ACOS(config-policy-class-list:example-cli...)# over-limit-
action forward log
```

Example

These commands configure a PBSLB template and bind it to a virtual port:

```
ACOS(config)# slb template policy bw1
ACOS(config-policy)# bw-list name bw1
ACOS(config-policy)# bw-list id 2 service srvcgroup2
ACOS(config-policy)# bw-list id 4 drop
ACOS(config-policy)# exit
ACOS(config)# slb virtual-server PBSLB_VS1 10.10.10.69
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-port)# template policy bw1
```

Example

The following example configures a bandwidth limit per source IP, using a policy template and class list.

Configure the class list:

```
ACOS(config)# class-list clist1
```

```
ACOS(config-class list)# 100.100.1.1/24 lid 1
ACOS(config-class list)# exit
```

Configure the PBSLB template:

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# class-list clist1
ACOS(config-policy-class-list:clist1)# lid 1
```

Configure the bandwidth limit (1 MB per second), and reset the connection when the limit is exceeded.

```
ACOS(config-policy-class-list:clist1-lid:1)# bw-rate-limit
1000 per 10
ACOS(config-policy-class-list:clist1-lid:1)# over-limit-action
reset
```

acos-event-log

Description Enable ACOS event logging in the forward policy of an SLB policy template.

Syntax

```
[no] acos-event-log
```

Mode SLB policy template under forward-policy

Example Enable this feature.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# acos-event-log
```

action

Description Specifies the ACOS behavior when a request matches the class list entry for servers using the template.

Syntax

```
[no] action MATCH-ACTION [LOG-TYPE]
```

Parameter	Description
MATCH-ACTION	Specifies the behavior. Valid options include: • **service-group***grp-name*-request is forwarded to

Parameter	Description
	specified service group. • **reset**- ACOS sends RST to the • **drop**- ACOS drops the request
LOG-TYPE	Specifies the log messages generated when a request matches the class list. Valid options include. • <no parameter> - no entries are logged • **logging 0** actions are immediately logged • **logging** <1 to 60> event are logged at the specified interval (minutes). Default value is three. • **logging fail** only unsuccessful connections are logged.

Mode SLB policy template class-list LID

Example This example configures the device to forward matching requests to the service group gp1 and create a log entry every 15 minutes.

```
ACOS(config)# slb template policy pol1
ACOS(config-policy)# class-list clist1
ACOS(config-policy-class-list:clist1)# lid 1
ACOS(config-policy-class-list:clist1-lid:1)# action service-
group group1 logging 15
ACOS(config-policy-class-list:clist1)# end
```

The show class-list command provides a hitcount parameter that displays the number of times a class list LID is matched:

```
ACOS# show class-list clist1
Name:                clist1
Total single IP:     2
Total IP subnet:     1
Content:
    1.1.1.1/32 lid 3 hitcount 0
    1.1.1.2/32 lid 2 hitcount 0
    13.13.13.0/24 lid 1 hitcount 3
```

bw-list id

Description Specifies the action to take for clients using a Black/White list ID.

Syntax

```
[no] bw-list id id {service-group name | drop | reset}
[logging [minutes] [fail]}
```

Parameter	Description
id	Group ID in the Black/White list (0-1023).
name	Sends clients to the SLB service group with the specified name on the ACOS device.
drop	Drops connections for IP addresses that are in the specified group.
reset	Resets connections for IP addresses that are in the specified group.
logging	Enables logging. The *minutes* option specifies how often messages can be generated. This option reduces overhead caused by frequent recurring messages. For example, if the logging interval is set to 5 minutes, and the PBSLB rule is used 100 times within a five-minute period, the ACOS device generates only a single message. The message indicates the number of times the rule was applied since the last message. You can specify a logging interval from 0 to 60 minutes. To send a separate message for each event, set the interval to 0. PBSLB rules that use the **service-group** *name* option also have a **fail** option for logging. This option configures the ACOS device to generate log messages only when there is a failed attempt to reach a service group. Messages are not generated for successful connections to the service group. The **fail** option is disabled by default. The **fail** option is not available for rules with the **drop** or **reset** option, since any time a drop or reset rule affects traffic, this indicates a failure condition.

Parameter	Description
	Logging is disabled by default. If you enable it, the default is 3 minutes.

Mode SLB policy template

Example Drop connections for clients matching Black/White list 3.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# bw-list id 3 drop
```

bw-list name

Description Binds the specified Black/White list to the virtual ports that use this template.

Syntax

```
[no] bw-list name name
```

Parameter	Description
name	Black/White list file name.

Mode SLB policy template

Example Bind the Black/White list “example-bw-list” to virtual ports using this template.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# bw-list name example-bw-list
```

bw-list over-limit

Description Specifies the action to take for traffic that is over the limit.

Syntax

```
[no] bw-list over-limit {lockup lock-min | logging log-min | reset}
```

Parameter	Description
lock-min	Do not accept any new connections for the specified number of minutes (1-127).
log-min	Generates a log message when traffic goes over the

Parameter	Description
	limit. This option specifies the log interval and can be 1-255 minutes.
`reset`	Resets new connections until the number of concurrent connections on the virtual port falls below the connection limit.

Default Drop

Mode SLB policy template

Usage The over-limit rule in a system-wide PBSLB policy includes an optional lockup period. If the lockup period is configured, the ACOS device continues to enforce the over-limit action for the duration of the lockup.

For example, if the over-limit action is drop, and a client exceeds the connection limit that is specified in the Black/White list, the ACOS device continues to drop all connection attempts from the client until the lockup expires.

By default, the **`lockup`** option is disabled. To enable it, you must specify a lockup period of 1-127 minutes.

The dynamic Black/White-list entry for a client does not age while the client is locked up. After the lockup ends, the timeout for the entry is reset to its full value and begins decreasing.

Example When traffic goes over the limit, do not accept any new connections for five minutes.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# bw-list over-limit lockup 5
```

bw-list timeout

Description Number of minutes dynamic Black/White-list client entries can remain idle before aging out.

Syntax

```
[no] bw-list timeout num
```

Parameter	Description
num	Number of minutes (1-127).

Default 5 minutes

Mode SLB policy template

Example Configure the timeout to 7 minutes.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# bw-list timeout 7
```

bw-list use-destination-ip

Description Matches Black/White list entries based on the client's destination IP address, instead of matching by client source address. Generally, this option is applicable when wildcard VIPs are used.

Syntax

```
[no] bw-list use-destination-ip
```

Default Disabled by default; the ACOS device matches by client source IP address.

Mode SLB policy template

Example Enable this feature.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# bw-list use-destination-ip
```

bw-rate-limit

Description Configure the bandwidth rate limit for servers that use this template.

Syntax

```
[no] bw-rate-limitnum-bytespernum-100ms
```

Parameter	Description
num-bytes	Rate limit in bytes (1-2147483647).
num-100ms	Rate interval in number of 100ms increments (1-65535).

Mode SLB policy template class-list LID

Example This example configures a bandwidth rate limit of 1,024,000 bytes per second (10 100ms intervals):

```
ACOS(config)# slb template policy pol1
ACOS(config-policy)# class-list clist1
ACOS(config-policy-class-list:clist1)# lid 1
ACOS(config-policy-class-list:clist1-lid:1)# bw-rate-limit
1024000 per 10
```

class-list

Description Create a class-list or geo-location class-list within the template.

Syntax

```
[no] class-list name
```

Parameter	Description
name	Name of the class-list (1-63 characters).

This command places you in a sub-configuration mode, where the following additional commands are available:

Command	Description
[no] client-ip {l3-dest | l7-header [*name*]}	Specifies the IP address to use for matching entries in an IP class list. l3-dest Matches based on the destination IP address in packets from clients. l7-header [*name*] Matches based on the IP address in the specified header *name* in packets from clients. If you do not specify a header *name*, the X-Forwarded-For header is used. This is available only with **request-limit** and **request-rate-limit**. By default, the client's IP address is used.
[no] lid	Adds a Limit ID (LID) entry to the class list, to specify

Command	Description
num	traffic limits for client traffic. Value of *num* ranges from 1 to 1023.

Mode SLB policy template

Usage The class-list **request-limit** and **request-rate-limit** options apply only to HTTP, fast-HTTP, and HTTPS virtual ports.

These options, when configured in a policy template, are applicable only in policy templates that are bound to virtual ports. These options are not applicable in policy templates bound to virtual servers (rather than individual ports).

The **over-limit-action log** option, when used with **request-limit** or **request-rate-limit**, always lists Ethernet port 1 as the interface.

conn-limit

Description Specifies the maximum number of concurrent connections allowed for a client.

Syntax

```
[no] conn-limit num
```

Parameter	Description
num	Maximum number of concurrent connections allowed (0-1048575). Connection limit 0 immediately locks down matching clients.

Mode SLB policy template class-list LID

Example This example configures a connection limit of 10000 concurrent connections.

```
ACOS(config)# slb template policy pol1
ACOS(config-policy)# class-list clist1
ACOS(config-policy-class-list:clist1)# lid 1
ACOS(config-policy-class-list:clist1-lid:1)# conn-limit 10000
```

conn-rate-limit

Description Specifies the maximum number of new connections allowed for a client within the specified limit period.

Syntax

```
[no] conn-rate-limit num-conn per num-100ms
```

Parameter	Description
num-conn	Maximum number of new connections allowed (1-2147483647).
num-100ms	Interval in number of 100ms increments (1-65535).

Mode SLB policy template class-list LID

Example This example configures 1,000,000 new connections allowed per second (10 100ms intervals):

```
ACOS(config)# slb template policy pol1
ACOS(config-policy)# class-list clist1
ACOS(config-policy-class-list:clist1)# lid 1
ACOS(config-policy-class-list:clist1-lid:1)# conn-rate-limit
1000000 per 10
```

forward-policy

Description Configure a forward policy of an slb policy template to specify permitted traffic destinations and sources along with the actions to apply. Forward policy is a required component when configuring an explicit HTTP proxy.

Syntax

```
[no] forward-policy
```

This command changes the CLI to forward-policy configuration mode, where the commands in Commands in the forward-policy Configuration Mode are available:

Table 22 : Commands in the forward-policy Configuration Mode

Command	Description
acos-event-log	Enable ACOS event logging.

Table 22 : Commands in the forward-policy Configuration Mode

Command	Description
`action` *`action-name`*	Specify the action policy name. This command places you in a sub-configuration mode, where the commands in Table 23 are available.
`local-logging`	Enable local logging.
`dual-stack-action`*`action-name`*	Configure this action to forward requests via IPv4 and IPv6 dual-stacked networks. Specify the action policy name. This command places you in a sub-configuration mode, where the commands in Table 25 are available.
`enable-adv-match`	Enable advanced mode to configure advanced match conditions for forward-policy. **Additional Notes:** • These conditions are available only in the **`destination adv-match`** rule and apply to HTTP or HTTPS virtual ports. • Enabling this command deactivates all the other kinds of destination rules. • Binding or switching the advanced mode forward-policy template on a virtual port enables **`proxy-layer v2`** implicitly.
`forward-http-connect-to-icap reqmod-icap` *`tem-plate-name`*	Command in forward-policy configuration mode to forward HTTP CONNECT request to ICAP server based on the specified slb template reqmod-icap. This enables the ICAP reqmod service to process the request before sending the request to the forward proxy. This option does not support the ICAP "preview" option. If this option is configured and bound to a virtual port, the “allowed-http-methods” and “min-

Table 22 : Commands in the forward-policy Configuration Mode

Command	Description
	payload-size" options defined in the `slb template reqmod-icap` are ignored.
`no-client-conn-reuse`	Inspects only the first request of a connection. Command in forward-policy configuration mode that dictates that the HTTP/HTTPS client will not send multiple requests to different destinations over the same TCP connection between the client and the ACOS. **NOTE:** In the case of a transparent proxy with SSL or SSLi, the **`no-client-conn-reuse`** command is not supported.
`require-web-category`	Command in forward-policy configuration mode enabling Web Category Lookup Enforcement web-category and web-reputation. Web category lookup enforcement resolves the category and reputation score of the unknown (first request) URLs by pausing the data plane connection. The connection is resumed when the result is known, and the URL is categorized or reputed.
`source` *`source-name`*	Command in forward-policy configuration mode to specify match rules for traffic sources and destination rules to define what destinations clients can access. Multiple source rules may be defined, but only a single source rule of **`match-any`** may be defined. This command places you in a sub-configuration mode, where the commands in Sub-Commands in the forward-policy source Configuration Mode are available.
`ssli-url-filtering`	Command in forward-policy configuration mode to change default actions related to the ACOS being

Table 22 : Commands in the forward-policy Configuration Mode

Command	Description
`{bypassed-sni-disable | intercepted-sni-enable | intercepted-http-disable | no-sni-allow}`	used as a transparent proxy in SSLi. The following options are available for this command at this level: • `bypassed-sni-disable` By default, an SNI extension inspection is done on bypassed transparent proxy SSLi traffic. Use this parameter to disable SNI inspection on bypassed traffic. • `intercepted-sni-enable` By default, intercepted traffic is inspected only at the HTTP header level. Use this parameter to enable SNI matching for intercepted transparent proxy SSLi traffic. • `intercepted-http-disable` By default, intercepted transparent proxy SSLi traffic has the HTTP header inspected. Use this parameter to disable http header inspection for intercepted transparent proxy SSLi traffic. • `no-sni-allow` By default, if SNI filtering is enabled for bypassed or intercepted connections, and an SNI extension is not present, the packet is dropped. Use this parameter to forward requests if an SNI extension is not found for transparent proxy SSLi traffic.
`ssli-url-filtering-san {enable-san |`	Command in forward-policy configuration mode to configure a SAN filtering on the transparent proxy in SSLi. The following options are available for this

Table 22 : Commands in the forward-policy Configuration Mode

Command	Description
`bypassed-san-disable | intercepted-san-enable | no-san-allow}`	command at this level: • `enable-san` Without SNI, if the **`no-sni-allow`** command is configured, SAN filtering is enabled for bypassed or intercepted connections. Use this parameter to allow SAN to filter on transparent proxy SSLi traffic. • `bypassed-san-disable` By default, a SAN extension inspection is done on bypassed transparent proxy SSLi traffic. Use this parameter to disable SAN inspection on bypassed traffic. • `intercepted-san-enable` By default, the intercepted traffic is not inspected for transparent proxy SSLi traffic. Use this parameter to enable SAN matching for intercepted transparent proxy SSLi traffic. • `no-san-allow` By default, if SAN filtering is enabled for bypassed or intercepted connections, and no SAN extension is present, the packet is dropped. Use this parameter to forward requests if SAN extension is not found for transparent proxy SSLi traffic.

Table 23 : Sub-Commands in the forward-policy action Configuration Mode

Command	Description
`[no] drop`	Sub-command in forward-policy-action

Table 23 : Sub-Commands in the forward-policy action Configuration Mode

Command	Description
	configuration mode to drop traffic.
`[no] drop-message` *text*	Sub-command in forward-policy-action configuration mode. Following the `drop` command, specify a message to appear. A default "Access to this site is blocked by administrator" message appears if nothing is specified. Commands `drop-message` and `drop-redirect-url` are mutually exclusive actions. If both are entered, the prior command will be overwritten by the more recent one. The command **`drop-message`** is not supported with SNI filtering.
`[no] drop-redirect-url` *url* `http-status-code` *http-status-code*]	Sub-command in forward-policy-action configuration mode. Following a `drop` command, specify a URL to redirect to after a client's request is dropped. The http-status-code default is 302 Found. Commands `drop-message` and `drop-redirect-url` are mutually exclusive actions. If both are entered, the prior command will be overwritten by the more recent one. The command **`drop-redirect-url`** is not supported with SNI filtering.
`[no] drop-response-code`	Specify a response code for drop action. The code range <100-599>.
`[no] log`	Sub-command in forward-policy-action configuration mode to provide log of actions taken.
`[no] sampling-`	Sub-command in forward-policy-action

Table 23 : Sub-Commands in the forward-policy action Configuration Mode

Command	Description
`enable {all | hits}`	configuration mode. Specify sampling-enable to enable baselining for all requests or for requests that match the destination rule.
`[no] forward-to-internet` *`fwd-sg`* `[snat` *`snat-pool-name`* `| port-translation-only] [fallback` *`fallback-sg`* `[snat` *`fb-snat-pool-name`* `| port-translation-only]`	Sub-command in forward-policy-action configuration mode to specify the service-group name to send internet traffic to. The following options are available in this command: • `snat` *`snat-pool-name`* Parameters that apply a configured source NAT. • `port-translation-only` Parameters that apply a configured source NAT to use source port translation only. • `fallback` *`fallback-sg`* Parameters that specify a service-group to send requests to for approved destinations that the ACOS device cannot resolve. • `snat` *`fb-snat-pool-name`* Parameters that apply a configured source NAT for fallback requests.
`[no] forward-to-service-group` *`fwd-sg`* `[snat` *`snat-pool-name`* `| port-translation-only]`	Sub-command in forward-policy-action configuration mode to specify the service-group to send service-group traffic to. The following options are available in this command: • `snat` *`snat-pool-name`* Parameters that apply a configured source NAT.

Table 23 : Sub-Commands in the forward-policy action Configuration Mode

Command	Description
	• `port-translation-only` Parameters that apply a configured source NAT to use source port translation only.
`forward-to-proxy` *`fwd-sg`* `[snat` *`snat-pool-name`* `| port-translation-only} ][bypass | support-cert-fetch]`	Sub-command in forward-policy-action configuration mode to specify the service-group to send HTTP proxy server traffic. This chains an ACOS device to an upstream proxy server when ACOS acts as a proxy. The following options are available in this command: • `snat` *`snat-pool-name`* Parameters that apply a configured source NAT. • `port-translation-only` Parameters that apply a configured source NAT to use source port translation only. • `bypass` Set this option to directly send all the HTTPS traffic to the upstream proxy. • `support-cert-fetch` Set this option for the server certificate to fetch the traffic and forward it through the explicit proxy instead of the real server as the original SSLi.

Table 24 : Sub-Commands in the forward-policy source Configuration Mode

Command	Description
`[no] destination adv-`	Sub-command in forward-policy-

Table 24 : Sub-Commands in the forward-policy source Configuration Mode

Command	Description
`match {priority num} {options}`	source configuration mode to specify the destination rule and advanced match-type for HTTP requests. Additional Notes: • Ensure that the `enable adv-match` command in the forward-policy configuration mode is already configured. • All forward-policy rules must include an `action` or a `dual-stack-action`. • If the match condition is unavailable in the current HTTP request, then ACOS will use 0 or an empty string as the default value. For example, if the The following options are available in this command: • `priority num` - Define the priority number to determine which rule to use when multiple matches occur. 1 is the lowest, and 1000 is the highest priority. The matched rule's priority number is displayed in the show log output. • `options` - Bind the actions and match-type options in the destination adv-match rule. See Table 25.

Table 24 : Sub-Commands in the forward-policy source Configuration Mode

Command	Description
`[no] destination any {action action-name | sampling-enable {all | hits}}`	Sub-command in forward-policy-source configuration mode to specify the destination rule to default to for requests. The following options are available in this command: • `action action-name` Specify the action to take for requests not defined. • `sampling-enable {all | hits}` Specify sampling-enable to enable baselining for all requests or for requests that match the destination rule.
`[no] destination class-list class-list- name | web-category-list web-category-list-name | web-reputation-scope reputation-scope} {action action-name} {host |ip | url} {priority priority-num} [sampling-enable {all | hits}]`	Sub-command in forward-policy-source configuration mode to specify the destination to send Internet traffic to, based on the following options: • `class-list class-list-name` Specify the allowed class-list to apply your action to. An Aho-Corasick or IP type class list may be used. • `web-category-list web-category-list-name` Specify the web-category-list to apply your action to. • `web-reputation-scope reputation-scope`

Table 24 : Sub-Commands in the forward-policy source Configuration Mode

Command	Description
	Specify the web-category reputation-scope for destination matching. • `action` *`action-name`* Specify the action to take for the previously defined class-list, web-category-list, and web-reputation. • `host | ip | url` Define whether a match should be based on the HTTP host header, layer 3 IP address, or HTTP URL. The `ip` parameter does not apply to `web-category-list` and `web-reputation` configuration. • `priority priority num` Define the priority by providing a number for the *priority num*. The number determines what rule to use when multiple matches occur. • `sampling-enable {all | hits}` Specify sampling-enable to enable baselining for all requests or for requests that match the destination rule.
`[no] match-any`	Sub-command in forward-policy-source configuration mode for

Table 24 : Sub-Commands in the forward-policy source Configuration Mode

Command	Description
	specifying a rule when there is no class-list, web-category list, or web-reputation scope match from defined sources.
`[no] match-authorize-policy` *`authoriz-policy-name`*	Specify an AAM authorization policy template to determine membership of users.
`[no] match-class-list` *`class-list`*	Sub-command in forward-policy-source configuration mode for specifying the IPv4 or IPv6 class-list name to use with the matching source rule. Specify the *`class-list`* to match the source rule; multiple class-lists can be specified by using one command per class-list.
`[no] priority` *`num`*	Specify a source's priority for aam authorization policy checking. The highest priority that may be defined is 1024. Each priority must have a unique value.
`[no] sampling-enable {all | destination-match-not-found | hits | no-host-info}...`	Sub-command in forward-policy-source configuration mode to specify baselining. The following options are available in this command at this level: • `all` Gather all the number of requests. • `hits`

Table 24 : Sub-Commands in the forward-policy source Configuration Mode

Command	Description
	Gather a number of requests that match the defined source rule. • `destination-match-not-found` Gather the number of requests with no matching destination rule. • `no-host-info` Gather number of requests that failed to parse ip or host information.

Table 25 : Sub-Commands in the dual-stack-action Configuration Mode

Command	Description
`[no] fallback`*`fall-back-sg`*`snat`*`fb-snat-pool-name`*	Sub-command in dual-stack-action configuration mode for specifying a service-group (*`fallback-sg`*) to send requests to approved destinations that the ACOS device cannot resolve. `snat`*`fb-snat-pool-name`* - Parameter to specify a source NAT pool or pool group for fallback requests.
`[no] ipv4`*`ipv4-sg`*`snat`*`ipv4-snat-pool-name`*	Sub-command in dual-stack-action configuration mode for specifying a service group to forward IPv4 requests. `snat`*`ipv4-snat-pool-name`* - Parameter to specify a source NAT pool or pool group for the IPv4 requests.
`[no] ipv6`*`ipv6-sg`*`snat`*`ipv6-`	Sub-command in dual-stack-action configuration mode for specifying a service group to forward IPv6 requests.

Table 25 : Sub-Commands in the dual-stack-action Configuration Mode

Command	Description
snat-pool-name	snat*ipv6-snat-pool-name* - Parameter to specify a source NAT pool or pool group for the IPv6 requests.
[no] log	Enable logging for actions taken.
[no] sampling-enable { all | hits }	Enable baselining for all requests or for requests that match the destination rule.

Table 26 : Sub-commands for destination adv-match options

Command	Description
action *action-name*	Specify the action to be taken for requests not defined. See Table 23.
disable-req-mod-icap	Disable the REQMOD ICAP template of a virtual port when the HTTP request matches the forward-policy rule.
disable-respmod-icap	Disable the RESPMOD ICAP template of a virtual port when the HTTP request matches the forward-policy rule.
dual-stack-action *action-name*	Configure this action to forward requests via IPv4 and IPv6 dual-stacked networks. See Table 25.
match-host *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the host (HTTP) or SNI/SAN (SSL).
match-http-content-encoding *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the value of "Content-Encoding."
match-http-content-	Specify the HTTP content-length range. You can specify 0-2147483647 bytes.

Table 26 : Sub-commands for destination adv-match options

Command	Description
`length-range` *num* `to` *num*	Take the required action when the HTTP request matches the value of "Content-Length" with an inclusive range.
`match-http-content-type` *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the "Content-Type."
`match-http-header` *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the name of all the request headers. **NOTE:** ACOS does not consider 'HOST' as a 'http-header.'
`match-http-method-connect`	Take the required action when the HTTP request matches the CONNECT method.
`match-http-method-delete`	Take the required action when the HTTP request matches the DELETE method.
`match-http-method-get`	Take the required action when the HTTP request matches the GET method.
`match-http-method-head`	Take the required action when the HTTP request matches the HEAD method.
`match-http-method-options`	Take the required action when the HTTP request matches the OPTIONS method.
`match-http-method-patch`	Take the required action when the HTTP request matches the PATCH method.
`match-http-method-post`	Take the required action when the HTTP request matches the POST method.
`match-http-`	Take the required action when the HTTP request matches the PUT

Table 26 : Sub-commands for destination adv-match options

Command	Description
`method-put`	method.
`match-http-method-trace`	Take the required action when the HTTP request matches the TRACE method.
`match-http-request-file-extension` *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the file extension of the URL in the HTTP request line.
`match-http-url` *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the URL in the HTTP request line.
`match-http-url-regex` *string-regex*	Specify the regular expression. Take the required action when the HTTP request line matches the URI with the specified regular expression. **NOTE:** When configuring the regular expression for this option, the characters "?", "*", "+", and "{0}" cannot be used as part of the regex pattern. These characters function as quantifiers in the regex library, and their standalone use can cause the regex compilation to fail.
`match-http-user-agent` *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the value of the HTTP header "User-Agent."
`match-server-address` *list-name*	Specify the name of the class-list. Take the required action when the HTTP request matches the target server IP address.
`match-server-port` *num*	Specify the server port number. You can specify in the range 1-65535.

Table 26 : Sub-commands for destination adv-match options

Command	Description
	Take the required action when the HTTP request matches the target server port number.
`match-server-port-range` *num to num*	Specify the server port number range. You can specify in the range 1-65535. Take the required action when the HTTP request matches the target server port range inclusively.
`match-time-range` *name*	Specify the name of the time-range that was defined in slb forward-proxy. Take the required action when the HTTP request matches the time-range rule.
`match-web-category-list` *name*	Specify the name of the `web-category-list` that was defined in the forward-policy. Take the required action when the HTTP request matches the time-range rule.
`match-web-reputation-scope` *name*	Specify the name of the `web-reputation-scope` that is defined in the forward-policy. Take the required action when the HTTP request matches the time-range rule.
`notify-page` *name*	Specify the name of the notify-page that was defined in slb forward-proxy. Take the required action when the HTTP request matches the notify-page rule.

Mode SLB policy template

Usage The **`forward policy action`** command defines actions that can be taken, and is normally used in conjunction with **`forward-policy source`** rules that link destination and matching rules for an **`slb template policy`**.

```
forward-to-internet fw-sg is just a placeholder.
```

Example Configure the action list Default_Deny to drop packets

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# action Default_Deny
ACOS(config-policy-forward-policy-action)# drop
```

Example Configure the source list `Any_Source` to apply the `Default_Deny` action for any requests that are not defined by a class-list or web-category-list or web-reputation-scope.

```
ACOS(config-policy-forward-policy)# source Any_Source
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination any
action Default_Deny
```

Example Configure the source `s1` to match IPs from class-list `Src-List` and links the destinations from `class-list dest` with rules to apply from the a1 action sub template, using a url check with a priority of `10`.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# source s1
ACOS(config-policy-forward-policy-source)# match-class-list
Src-List
ACOS(config-policy-forward-policy-source)# destination class-
list dest action a1 url priority 10
```

Example Configure the **`dual-stack-action`** to forward requests via IPv4 and IPv6 networks.

```
ACOS(config)# slb template policy DUAL_Stack_6n4
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# dual-stack-action FWD_6n4
ACOS(config-policy-forward-policy-dual-st...)# ipv4 To_
Internet_v4 snat EP_POOL_v4
ACOS(config-policy-forward-policy-dual-st...)# ipv6 To_
Internet_v6 snat EP_POOL_v6
ACOS(config-policy-forward-policy-dual-st...)# fallback To_
Internet_v6 snat fall_back_v6
ACOS(config-policy-forward-policy-dual-st...)# log
```

Bind the **`dual-stack-action`** to any destination rule of the forward policy.

```
ACOS(config-policy-forward-policy)# source ANY
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination any
dual-stack-action FWD_6n4
```

Example Configure the **forward-policy** to enable the advance match for the destination rule.

```
ACOS(config)# slb template policy ICAP_test
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# enable-adv-match
ACOS(config-policy-forward-policy)# action FWD
```

Bind the **adv-match** option to the destination rule and disable the REQMOD and RESPMOD ICAP templates when the HTTP request meets the conditions.

```
ACOS(config-policy-forward-policy)# source ICAP_TEST
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination adv-
match 1000
ACOS(config-policy-forward-policy-source-...)# match-http-
content-length-range 1048576 to 0
ACOS(config-policy-forward-policy-source-...)# disable-reqmod-
icap
ACOS(config-policy-forward-policy-source-...)# disable-
respmod-icap
ACOS(config-policy-forward-policy-source-...)# action FWD
```

forward-policy action

Description Specify the action in the forward policy of SLB policy template.

Syntax

```
[no] action action-name {drop | drop-message | drop-redirect-
url | drop-response-code | sampling-enable | log | forward-to-
internet | forward-to-service-group | forward-to-proxy }
```

Parameter	Description
action-name	Specify the action policy name.
[no] drop	Drop the traffic in forward-policy actions.

Parameter	Description
[no] drop-message *text*	Specify a message to appear after the message is dropped. The default message is: “Access to this site is blocked by administrator”. **NOTE:** This command is not supported with SNI filtering.
[no] drop-redirect-url *url*[**http-status-code**] *http-status-code*	Specify a URL to redirect to after a client’s request is dropped along with the status code. The default http-status-code is '302 Found'. **NOTE:** This command is not supported with SNI filtering. Commands **drop-message** and **drop-redirect-url** are mutually exclusive actions. If both are entered, the prior command will be overwritten by the more recent one.
[no] drop-response-code	Specify response code for drop action. The code range <100-599>.
[no] log	Enable logging for actions taken.
[no] sampling-enable {all | hits}	Enable baselining for all requests or for requests that match the destination rule.
[no] forward-to-internet*fwd-sg*	Specify the service-group name to send internet traffic to. The following options are available in this command:
snat *snat-pool-name*	Parameters that apply a configured source NAT.
fallback *fallback-sg*	Parameters that specify a service-group to send requests to for approved destinations that the

Parameter	Description
	ACOS Device device cannot resolve .
snat *fb-snat-pool-name*	Parameters that apply a configured source NAT for fallback requests.
[no] forward-to-service-group *fwd-sg*	Specify the service-group to send service-group traffic to. The following options are available in this command:
snat *snat-pool-name*	Parameters that apply a configured source NAT.
forward-to-proxy *fwd-sg*	Specify the service-group to send HTTP proxy server traffic. This chains an ACOS device to an upstream proxy server when ACOS acts as a proxy. The following options are available in this command:
snat *snat-pool-name*	Parameters that apply a configured source NAT.
bypass	Set this option to send all the HTTPS traffic to upstream proxy directly.
support-cert-fetch	Set this option for the server certificate to fetch the traffic and forward it through the explicit proxy instead of the real server as the original SSLi.

Mode SLB policy template

Usage The forward-policy action command defines actions that can be taken, and is normally used in conjunction with forward-policy source rules that link destination and matching rules for an **slb template policy**.

Example Configure the action list Default_Deny to drop packets

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# action Default_Deny
ACOS(config-policy-forward-policy-action)# drop
```

Example Configure the source list `Any_Source` to apply the `Default_Deny` action for any requests that are not defined by a class-list or web-category-list or web-reputation-scope.

```
ACOS(config-policy-forward-policy)# source Any_Source
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination any
action Default_Deny
```

Example Configure the source `s1` to match IPs from class-list `Src-List` and links the destinations from `class-list dest` with rules to apply from the a1 action sub template, using a url check with a priority of `10`.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# source s1
ACOS(config-policy-forward-policy-source)# match-class-list
Src-List
ACOS(config-policy-forward-policy-source)# destination class-
list dest action a1 url priority 10
```

forward-policy source

Description specify match rules for traffic sources and destination rules to define what destinations clients are allowed to access. Multiple source rules may be defined, but only a single source rule of **match-any** may be defined.

Syntax

```
[no] source source-name
```

Command	Description
source-name	Specify the name of source.
[no] destination any {action *action-name* | **sampling-enable {all | hits}**}	Specify the destination rule to default to for requests. The following options are available in this command level: • **action** *action-name*

Command	Description
	Specify the action to take for requests not defined. • **sampling-enable {all | hits}** Specify sampling-enable to enable baselining for all requests or for requests that match the destination rule.
[no] destination	Specify the destination to send Internet traffic to. The following options are available in this command level:
class-list *class-list-name*	Specify the allowed class-list to apply your action to. An Aho-Corasick or IP type class list may be used.
web-category-list *web-category-list-name*	Specify the web-category-list to apply your action to.
web-reputation-scope *reputation-scope*	Specify the web-category reputation-scope for destination matching.
action *action-name*	Specify the action to take for the previously defined class-list, web-category-list, and web-reputation.
host | ip | url	Define if a match should be based on the HTTP host header, or layer 3 IP address, or HTTP URL. The `ip` parameter is not applicable to `web-category-list` and `web-reputation` configuration.
priority *priority-num*	Define the priority by providing a number for *priority num*. The number determines what rule to use when multiple matches

Command	Description
	occur.
sampling-enable {all | hits}	Specify sampling-enable to enable baselining for all requests or for requests that match the destination rule.
[no] match-any	Specify a rule when there is no class-list or web-category list or web-reputation scope match from defined sources.
[no] match-authorize-policy *authoriz-policy-name*	Specify an aam authorization policy template to determine membership of users.
[no] match-class-list *class-list*	Specify the IPv4 or IPv6 class-list name to use with the matching source rule. Specify the *class-list* to match the source rule; multiple class-lists can be specified by using one command per class-list.
[no] priority *num*	Specify a source's priority for aam authorization policy checking. The highest priority that may be defined is 1024. Each priority must have a unique value.
[no] sampling-enable	Specify the baselining for the source. The following options are available in this command level:
all	Gather the number of all requests.
destination-match-not-found	Gather the number of requests with no matching destination rule.
hits	Gather the number of requests that match the defined source rule.
no-host-info	Gather number of requests that failed to parse IP or host information.

Mode SLB policy template

Usage The **forward policy** forward-policy action command defines actions that can be taken, and is normally used in conjunction with **forward-policy source** rules that link destination and matching rules for an **slb template policy**.

Example Configure the action list Default_Deny to drop packets

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# action Default_Deny
ACOS(config-policy-forward-policy-action)# drop
```

Example Configure the source list Any_Source to apply the Default_Deny action for any requests that are not defined by a class-list or web-category-list or web-reputation-scope.

```
ACOS(config-policy-forward-policy)# source Any_Source
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination any
action Default_Deny
```

Example Configure the source s1 to match IPs from class-list Src-List and links the destinations from class-list dest with rules to apply from the a1 action sub template, using a url check with a priority of 10.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# source s1
ACOS(config-policy-forward-policy-source)# match-class-list
Src-List
ACOS(config-policy-forward-policy-source)# destination class-
list dest action a1 url priority 10
```

forward-policy ssli-url-filtering

Description Change default actions in the forward-policy related to the ACOS Device being used as a transparent proxy in SSLi.

Syntax

```
[no] ssli-url-filtering {bypassed-sni-disable | intercepted-
sni-enable |
intercepted-http-disable | no-sni-allow}
```

Parameter	Description
bypassed-sni-disable	By default, an SNI extension inspection is done on bypassed transparent proxy SSLi traffic. Use this parameter to disable SNI inspection on bypassed traffic.
intercepted-sni-enable	By default, intercepted traffic is inspected only at the HTTP header level. Use this parameter to enable SNI matching for intercepted transparent proxy SSLi traffic.
intercepted-http-disable	By default, intercepted transparent proxy SSLi traffic has the HTTP header inspected. Use this parameter to disable HTTP header inspection for intercepted transparent proxy SSLi traffic.
no-sni-allow	By default, if SNI filtering is enabled for bypassed or intercepted connections, and an SNI extension is not present, the packet is dropped. Use this parameter to allow requests to be forwarded if SNI extension is not found for transparent proxy SSLi traffic.

Mode SLB policy template

Example Configure this feature disable SNI inspection on bypassed traffic.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# ssli-url-filtering
bypassed-sni-disable
```

forward-policy ssli-url-filtering-san

Description Configure a SAN filtering on transparent proxy in SSLi..

Syntax

```
[no] ssli-url-filtering-san {enable-san | bypassed-san-disable
| intercepted-san-enable | no-san-allow}
```

Parameter	Description
enable-san	In the absence of SNI, if the **no-sni-allow** command is configured, the SAN filtering is enabled for bypassed or intercepted connections. Use this parameter to enable SAN filtering on transparent proxy SSLi traffic.
bypassed-san-disable	By default, a SAN extension inspection is done on bypassed transparent proxy SSLi traffic. Use this parameter to disable SAN inspection on bypassed traffic.
intercepted-san-enable	By default, the intercepted traffic is not inspected for transparent proxy SSLi traffic. Use this parameter to enable SAN matching for intercepted transparent proxy SSLi traffic.
no-sni-allow	By default, if SAN filtering is enabled for bypassed or intercepted connections, and there is no SAN extension present, the packet is dropped. Use this parameter to allow requests to be forwarded if SAN extension is not found for transparent proxy SSLi traffic

Mode SLB policy template

Example Configure this feature disable SNI inspection on bypassed traffic.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# ssli-url-filtering
bypassed-sni-disable
```

geo-location full-domain-tree

Description Checks current connection count for the client's specific geo-location and for all geo-locations higher up in the domain tree.

It is recommended to enable or disable this option before enabling GSLB. Changing the state of this option while GSLB is running can cause the related statistics counters to be incorrect.

Syntax `[no] geo-location full-domain-tree`

Default Disabled by default; when a client requests a connection, the ACOS device checks the connection count only for the specific geo-location level of the client. If the connection limit for that specific geo-location level has not been reached, the client's connection is permitted.

Mode SLB policy template

Example Enable this feature.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# geo-location full-domain-tree
```

geo-location overlap

Description Enables overlap matching mode. If there are overlapping addresses in the Black/White list or class list, use this option to enable the ACOS device to find the most precise match.

Syntax `[no] geo-location overlap`

Default Disabled

Mode SLB policy template

Example Enable this feature.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# geo-location overlap
```

geo-location share

Description Enables sharing of PBLSB statistics counters for virtual servers and virtual ports that use the template. This option causes the following counters to be shared:

- Permit
- Deny
- Connection number

- Connection limit

It is recommended to enable or disable this option before enabling GSLB. Changing the state of this option while GSLB is running can cause the related statistics counters to be incorrect.

Syntax `[no] geo-location share`

Default Disabled

Mode SLB policy template

Example Enable this feature.

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# geo-location share
```

over-limit-action

Description Specifies the action to take when a client exceeds one or more of the limits. The command also configures lockout and enables logging.

Syntax `[no] over-limit-action [forward | reset] [lockout minutes] [log minutes]`

Parameter	Description
drop	The ACOS device drops that traffic. If logging is enabled, the ACOS device also generates a log message. **NOTE:** There is no **drop** keyword; this is the default action.
forward	The ACOS device forwards the traffic. If logging is enabled, the ACOS device also generates a log message.
reset	For TCP, the ACOS device sends a TCP RST to the client. If logging is enabled, the ACOS device also generates a log message.
lockout	Specifies the number of minutes during which to apply the over-limit action after the client exceeds a limit. The lockout period is activated when a client exceeds any limit. The lockout period can be 1-1023 minutes.

Parameter	Description
log	Generates log messages when clients exceed a limit. When logging is enabled, a separate message is generated for each over-limit occurrence, by default. You can specify a logging period where the ACOS device holds the repeated messages for the specified period, then sends one message at the end of the period for all instances within the period. The logging period can be 0-255 minutes. The default is 0 (no wait period)

Mode SLB policy template class-list LID

request-limit

Description Specifies maximum number of concurrent Layer 7 requests allowed for a client.

Syntax

```
[no] request-limit num
```

Parameter	Description
num	Number of concurrent Layer 7 requests (1-1048575).

Mode SLB policy template class-list LID

request-rate-limit

Description Specifies the maximum number of Layer 7 requests allowed for the client within the specified limit period.

Syntax

```
[no] request-rate-limit num-req per num-100ms
```

Parameter	Description
num-req	Maximum number of new requests allowed (1-4294967295).
num-100ms	Interval in number of 100ms increments (1-65535).

Mode SLB policy template class-list LID

response-code-rate-limit

Description Configure a limit for the number of times a specified range of server response codes is received in a specified period of time.

NOTE: This feature only works for SMTP virtual ports. See the example below.

Syntax

```
[no] response-code-rate-limit
start-code-range-end-code-range num perseconds
```

Parameter	Description
start-code-range	Start rage of server response codes (100-600).
end-code-range	End range of server response codes (100-600).
num	Number of times there is a match on the specified response code(s).
seconds	Time limit interval, in seconds.

Mode SLB policy template class-list LID

Example This example configures a policy template with a response code rate limit and then applies the template to an SMTP virtual port. The response code rate limit will be exceeded when there are:

- 2 matches every 20 seconds for response codes numbered 500-590
- 15 matches per 127 seconds for response codes numbered 300-390

If either limit is exceeded, the **reset** action is applies fro 10 minutes and logged.

```
ACOS(config)# slb template policy pol1
ACOS(config-policy)# class-list clist1
ACOS(config-policy-class-list:clist1)# lid 1
ACOS(config-policy-class-list:clist1-lid:1)# over-limit-action
reset lockout 10 log
ACOS(config-policy-class-list:clist1-lid:1)# response-code-
rate-limit 500 - 590 2 per 20
ACOS(config-policy-class-list:clist1-lid:1)# response-code-
rate-limit 300 - 390 15 per 127
```

```
ACOS(config-policy-class-list:clist1-lid:1)#
end
ACOS# configure
ACOS(config)# slb virtual-server VS_SMTP1 10.5.5.10
ACOS(config-slb vserver-vport)# port 25 smtp
ACOS(config-slb vserver-vport)# template policy pol1
```

slb template port

Description Configure a template of SLB settings for service ports on real servers.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all virtual ports that use the template.

Syntax

```
[no] slb template port {default | template-name}
```

Parameter	Description
default	Edit the default port template. This template can be modified in the same way as any custom *template-name* you specify.
template-name	Template name (1-127 characters)

Mode Configuration mode

Usage The normal form of this command creates a real port template. The **no** form of this command removes the template.

You can bind only one real port template to a real port. However, you can bind the real port template to multiple real ports.

Some of the parameters that can be set using a template can also be set or changed on the individual port.

- If a parameter is set (or changed from its default) in both a template and on the individual port, the setting on the individual port takes precedence.

- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual port, the setting in the template takes precedence.

Example The following example configures a real port template named "common-rpsettings", enables slow-start in the template, and binds the template to a real port:

```
ACOS(config)#  slb template port common-rpsettings
ACOS(config-rport)# slow-start from 256
ACOS(config-rport)#  exit
ACOS(config)#  slb server rs1 10.1.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# template port common-
rpsettings
```

bw-rate-limit

Description Configure the bandwidth rate limit for ports that use this template.

Syntax

```
[no] bw-rate-limit limnum resume resnum duration durnum [no-
logging]
```

Parameter	Description
limnum	Bandwidth rate limit number in Kbps (1-16777216).
resnum	Resume port selection after bandwidth drops below this threshold, in Kbps (1-16777216).
durnum	Time period the rate limit needs to honor to both exceed bw-rate-limit number and drop below resume number, in seconds (1-250).
no-logging	Do not log bandwidth rate limit related state transitions.

Default Not set

Mode SLB port template

conn-limit

Description Maximum number of connections allowed on the port using this template.

Syntax

```
[no] conn-limit max-num [resume resume-num] [no-logging]
```

Parameter	Description
max-num	Maximum number of concurrent connections (1-64000000).
resume-num	Maximum number of connections the port can have before the ACOS device resumes use of the port (1-1048575).
no-logging	Disables logging for this feature.

Default 64000000 (64 million)

Mode SLB port template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure 7 million as the maximum number of connections, with no logging:

```
ACOS(config)# slb template port default
ACOS(config-rport)# conn-limit 7000000 no-logging
```

conn-rate-limit

Description Limits the rate of new connections the ACOS device is allowed to send to ports that use this template. When a port reaches its connection limit, the ACOS device stops selecting the port for client requests.

Syntax

```
[no] conn-rate-limit connections [per {100ms | second}] [no-logging]
```

Parameter	Description
connections	Maximum number of new connections allowed on a port. You can specify 1-1048575 connections.
per {**100ms** | **1sec**}	Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (1sec).
no-logging	Disable logging when this feature is enabled.

Default By default this is not set; when enabled, the default sampling rate is per 1sec.

Mode SLB port template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure 1 million as the maximum number of new connections per second, with no logging:

```
ACOS(config)# slb template port default
ACOS(config-rport)# conn-rate-limit 1000000 per second no-logging
```

dampening-flaps

Description Specifies parameters for taking a port or service group out of service when they report flaps. A flap is consecutive down and up status reports.

When the template is bound to a port or service-group and that entity reports more flaps than specified by the max parameter over the period

specified by flap-time, the entity is forced down and remains out of the rotation for the period specified by down-time.

Syntax

```
dampening-flaps max flap-period flap-time restore-svc-time
down-time
```

Parameter	Description
max	the number of flaps an entity can report during the flap period and remain in service. Flaps in excess of this number trigger a dampening event
flap-time	time period for counting flaps. Upon flap-time expiry, the flap count reset to zero.
down-time	time period the entity remains out of service

Default By default this is not set

Mode SLB port template

Example This example configures the template to force a port down if it experiences more than 3 flaps within 20 seconds. The entity remains out of service for 40 seconds.

```
ACOS(config)# slb template port PORT1
ACOS(config-rport)# dampening-flaps 3 flap-period 20 restore-
svc-time 40
```

del-session-on-server-down

Description This command clears a port protocol session within 2 to 3 seconds if a session server is disabled by ACOS command or the server fails an ACOS health check at the service group level.

If a one or more real servers in a service group fails the health check and this command is enabled for the session, ACOS clears the session.

Active sessions, (receiving client-side packets) are cleared within 2 to 3 seconds. Idle sessions may continue to exist for more than a minute after the command is issued.

Syntax

```
[no] del-session-on-server-down
```

Default This feature is disabled by default.

Mode SLB port template

Example This example shows how the command is applied:

```
ACOS(config)# slb template port default
ACOS(config-rport)# del-session-on-server-down
```

dest-nat

Description Enables destination Network Address Translation (NAT) on ports that use this template.

Destination NAT is enabled by default, but is automatically disabled in Direct Server Return (DSR) configurations. You can re-enable destination NAT on individual ports for deployment of mixed DSR configurations, which use backup servers across Layer 3 (in different subnets).

Syntax

```
[no] dest-nat
```

Default Disabled.

Mode SLB port template

Example Enable destination NAT on ports that use this template:

```
ACOS(config)# slb template port default
ACOS(config-rport)# dest-nat
```

down-grace-period

Description Number of seconds the ACOS device will continue to forward packets to a port that is down. This option is useful for taking servers down for maintenance without immediately impacting existing sessions on the servers. You can specify 1-86400 seconds.

NOTE: The service group must contain 2 or more servers for this feature to work.

This feature supports stateless and stateful load balancing. However, the feature is not supported for stateful hash load-balancing methods, such as source-IP-based or destination-IP-based hashing.

Syntax

```
[no] down-grace-period num
```

Parameter	Description
num	Number of seconds (1-86400).

Mode SLB port template

Example Set the grace period to 3600 seconds.

```
ACOS(config)# slb template port default
ACOS(config-rport)# down-grace-period 3600
```

dscp

Description Sets the differentiated services code point (DSCP) value in the IP header of a client request before sending the request to ports that use this template.

Syntax

```
[no] dscp num
```

Parameter	Description
num	DSCP value (1-63).

Default By default, DSCP is not set by the ACOS device.

Mode SLB port template

Example The following example illustrates how this feature works:

1. Configure a port template named `t1` that marks DSCP 4 on outgoing packets.

```
slb template port t1
  dscp 4
```

2. Configure a virtual-port template named `vp1` that marks DSCP 6 on outgoing packets.

```
slb template virtual-port vp1
  dscp 6
```

3. Bind `t1` to both `port 80 tcp` and `port 443 tcp`.

```
  slb server s1 9.8.8.15
  port 80 tcp
    template port t1
  port 443 tcp
    template port t1
```

4. Configure a virtual server named `vip2` with virtual `port 80 http` and `port 443 tcp`. Although the `vp1` template is bound to both ports, outgoing packets are marked with DSCP 4, because real ports take precedence over virtual ports.

```
  slb virtual-server vip2 fd5a:bfc:563c:bcda::100
  port 80 http
    source-nat pool s2
    service-group sg-80-6
      template virtual-port vp1
  port 443 https
    source-nat pool s2
    service-group sg-443-6
      template server-ssl s1
      template client-ssl cl-ssl1
      template virtual-port vp1
```

dynamic-member-priority

Description Configure service-group priority settings for ports on dynamically created servers. When configuring the service group, add the port template to the member.

Syntax

```
[no] dynamic-member-priority num decrement delta
```

Parameter	Description
num	Initial TTL for dynamically created service-group members (1-16).

Parameter	Description
	The default is 16.
delta	Amount to decrement the TTL if the IP address is not included in the DNS reply (0-7). The default is 0.

Mode SLB port template

Example Set the initial TTL to 12 and decrement value to 1.

```
ACOS(config)# slb template port default
ACOS(config-rport)# dynamic-member-priority 12 decrement 1
```

extended-stats

Description Enables collection of SLB peak connection statistics for the port.

Syntax

```
[no] extended-stats
```

Default Disabled.

Mode SLB port template

Example Enable this feature:

```
ACOS(config)# slb template port default
ACOS(config-rport)# extended-stats
```

health-check

Description Enables health monitoring of ports that use this template.

Syntax

```
[no] health-check name
```

Parameter	Description
name	Name of a configured health monitor.

Default By default, health checking is disabled.

Mode SLB port template

Usage If you omit this command or you enter it without the monitor-name option, the default TCP or UDP health monitor is used:

- TCP—Every 30 seconds, the ACOS device sends a connection request (TCP SYN) to the specified TCP port on the server. The port passes the health check if the server replies to the ACOS device by sending a TCP SYN ACK.
- UDP—Every 30 seconds, the ACOS device sends a packet with a valid UDP header and a garbage payload to the UDP port. The port passes the health check if the server either does not reply, or replies with any type of packet except an ICMP Error message.

Example Create health monitor “hm-dad” the enable health monitoring for ports using this template, using “hm-dad” as the health monitor.

```
ACOS(config)# health monitor hm-dad
ACOS(config-health:monitor)# disable-after-down
ACOS(config-health:monitor)# exit
ACOS(config)# slb template port default
ACOS(config-rport)# health-check hm-dad
```

health-check-disable

Description Disable health checking for the port.

Syntax

```
[no] health-check-disable
```

Default By default, health checking is disabled.

Mode SLB port template

Example Disable health checking:

```
ACOS(config)# slb template port default
ACOS(config-rport)# health-check-disable
```

inband-health-check

Description Supplements the standard Layer 4 health checks by using client-server traffic to check the health of service ports.

Syntax

```
[no] inband-health-check [down-timer seconds] [resel-on-reset]
[retry max-retries] [reassign max-reassigns]
```

Parameter	Description
seconds	Amount of time in seconds to bring up the server or port that is marked down (0-255). The default is 0; the server or port is never brought up.
resel-on-reset	When receiving a reset from server, also re-select the server and port. This is disabled by default.
max-retries	Each client-server session has its own retry counter. The ACOS device increments a session's retry counter each time a SYN ACK is late. If the retry counter exceeds the configured maximum number of retries allowed, the ACOS device sends the next SYN for the session to a different server. The ACOS device also resets the retry counter to 0. You can set the retry counter to 0-7 retries. The default number of retries is 2.
max-reassigns	Each real port has its own reassign counter. Each time the retry counter for any session is exceeded, the ACOS device increments the reassign counter for the server port. If the reassign counter exceeds the configured maximum number of reassignments allowed, the ACOS device marks the port down. In this case, the port remains down until the next time the port successfully passes a standard health check. Once the port passes a standard health check, the ACOS device starts using the port again and resets the reassign counter to 0. You can set the reassign counter to 0-255 reassignments. The default is 25 reassignments.

Default Disabled.

Mode SLB port template

Usage It is recommended that you continue to use standard Layer 4 health monitoring even if you enable in-band health monitoring. Without standard health monitoring, a server port marked down by an in-band health check remains down.

Example Enable inband health checking.

```
ACOS(config)# slb template port default
ACOS(config-rport)# inband-health-check down-timer 5 resel-on-reset
```

no-ssl

Description Disables SSL for server-side connections. This command is useful if a server-SSL template is bound to the virtual port that uses this real port, and you want to disable encryption on this real port.

Using the double-negative form of the command (**no no-ssl**) enables SSL for server-side connections..

Syntax

```
[no] no-ssl
```

Default Encryption is disabled by default, but it is enabled for server-side connections when the real port is used by a virtual port that is bound to a server-SSL template.

Mode SLB port template

Example Disable SSL for server-side connections:

```
ACOS(config)# slb template port default
ACOS(config-rport)# no-ssl
```

request-rate-limit

Description Limits the number of new requests that can be received by the port.

NOTE: This command applies only to configurations that use an external-service template.

Syntax

```
[no] request-rate-limit num
[per {100ms | second}] [reset] [no-logging]
```

Parameter	Description
num	Maximum number of new connection requests allowed per the specified interval (1-1048575).
per	Interval for the rate: • 100ms—Up to *num* new connection requests are allowed per one-tenth second (100-ms). • second—Up to *num* new connection requests are allowed per second.
reset	Sends a RST to a client that sends a new request during an interval in which the request rate has been exceeded. By default, requests that are received after the limit is exceeded are dropped with no RST.
no-logging	Disable logging for this feature.

Mode SLB port template

Example Set the request rate limit to 500,000 per 100ms.

```
ACOS(config)# slb template port default
ACOS(config-rport)# request-rate-limit 500000 per 100ms
```

slow-start

Description Provides time for real ports that use the template to ramp-up after TCP/UDP service is enabled, by temporarily limiting the number of new connections on the ports.

Syntax

```
[no] slow-start
[from start-conn-limit]
[times scale-factor | add conn-increment | every interval]
[till end-conn-limit]
```

Parameter	Description
start-conn-	Maximum number of concurrent connections to allow on the service port after it first comes up. You can

Parameter	Description
limit	specify from 1-4095 concurrent connections. The default is 128.
scale-factor	Number by which to multiply the starting connection limit. For example, if the scale factor is 2 and the starting connection limit is 128, the ACOS device increases the connection limit to 256 after the first ramp-up interval. The scale factor can be 2-10. The default is 2.
conn-increment	Number of additional concurrent connections to allow. You can specify 1-4095 new connections.
interval	Number of seconds between each increase of the number of concurrent connections allowed. For example, if the ramp-up interval is 10 seconds, the number of concurrent connections to allow is increased every 10 seconds. The ramp-up interval can be 1-60 seconds. The default is 10 seconds.
end-conn-limit	Maximum number of concurrent connections to allow during the final ramp-up interval. After the final ramp-up interval, the slow start is over and does not limit further connections to the server. You can specify from 1-65535 connections. The default is 4096.

Mode SLB port template

Example Configure ramp-up for ports; 128 connections to start, increase every 15 seconds, until 4096 connections are reached.

```
ACOS(config)# slb template port default
ACOS(config-rport)# slow-start from 128 every 15 till 4096
```

source-nat

Description Specifies the IP NAT pool to use for assigning source IP addresses to client traffic sent to ports using this template. When the ACOS device performs NAT for a port that is bound to the template, the device selects an IP address from the pool.

Syntax `[no] source-nat name`

Parameter	Description
name	Name of the configured NAT pool.

Mode SLB port template

Example Use “np1” as the source NAT pool.

```
ACOS(config)# slb template port default
ACOS(config-rport)# source-nat np1
```

stats-data-disable

Description Disables statistical data collection for ports that use this template..

Syntax `[no] stats-data-disable`

Default Stats collection is enabled by default.

Mode SLB port template

Example Disable statistical data collection:

```
ACOS(config)# slb template port default
ACOS(config-rport)# stats-data-disable
```

stats-data-enable

Description Enables statistical data collection for ports that use this template..

Syntax `[no] stats-data-enable`

Default Stats collection is enabled by default.

Mode This command is applicable to the following configuration modes

- SLB port template
- SLB server template
- Real server
- Service group
- Virtual server
- Virtual port

Example Enable statistical data collection:

```
ACOS(config)# slb template port default
ACOS(config-rport)# stats-data-enable
```

weight

Description Specifies the load-balancing preference for ports that use this template. A higher weight gives preference to the server and port relative to other servers and ports.

Syntax

```
[no] weight num
```

Parameter	Description
num	Specify the administrative weight assigned to the server. The value can be between 1-1000.

Default 1

Mode This command applies to the following modes:

- SLB port template
- SLB server template
- Real server

Usage This option applies only to the **service-weighted-least-connection** load-balancing method. This option does not apply to the **weighted-least-connection** or **weighted-round-robin** load-balancing methods.

Example Configure 3 as the weight in the SLB port template.

```
ACOS(config)# slb template port default
ACOS(config-rport)# weight 3
```

Example Configure 3 as the weight in the SLB server template.

```
ACOS(config)# slb template server default
ACOS(config-rserver)# weight 5
```

Example Configure 3 as the weight in the real server.

```
ACOS(config)# slb server 10.10.10.5
ACOS(config-real server)# weight 20
```

slb template quic

Description Configures a template for QUIC traffic load balancing.

Syntax

```
[no] slb template quic  template-name
```

Replace *template-name* with the name of the template, up to 31 characters.

This command enters the SLB QUIC Template Configuration mode where the following commands are available.

Parameter	Description
burst-len	
connection-id-length	Specify the QUIC connection ID length (in bytes) that ACOS can store. By default, the value is set to 3 bytes. The value can be between 1-20. The connection ID contains the details of the server ID. The ACOS device extracts the connection ID details and sends the traffic back to the back-end server.
idle-timeout	Specify the number of seconds a QUIC connection can remain idle before the ACOS device terminates the connection. By default, the value is set to 120 seconds. The value can be between 1-3600. This value is advertised to the endpoints. However, the actual value is the smallest value after negotiation. For example, if the idle timeout of the client or

Parameter	Description
	server is 60 and that of ACOS is 120, the connection will pick 60, and vice versa. ACOS acts as a proxy between the client and server, so two connections face each other, potentially with a different idle value. The rule is that when the client idle timeout expires, the server idle timeout also expires. Therefore, if the server idle timeout is earlier than the client side, it will not close the client connection.
key-update-to-client	Enable this command to initiate a key update from the ACOS side to the QUIC client.
key-update-to-server	Enable this command to initiate a key update from the ACOS side to the QUIC server.
receive-buf-fer	Specify the buffer size (in bytes) to control the window of the ACOS receiver. This number is used to raise the receive ceiling of the stream (MAX_STREAM_DATA). By default, the value is set to 20000 bytes. The value can be between 30000-400000.
server-retry	Enable this command for ACOS to send a retry packet to the QUIC client upon receiving the Initial packet.

Default NA

Mode SLB Template QUIC

Usage ACOS supports QUIC layer load balancing by leveraging several QUIC functionalities described in various RFCs, such as 8999, 9000, and 9001. ACOS acts as a proxy, routing, and load balancing QUIC packets from the client to the back-end servers.

The QUIC template is used to control the QUIC connection behavior. You can bind the slb quic template to the 'quic' and 'http-over-quic' virtual server ports.

Example The following commands configure the SLB template QUIC:

```
ACOS(config)# slb template quic http3_quic
ACOS(config-quic)# idle-timeout 200
ACOS(config-quic)# connection-id-length 20
ACOS(config-quic)# receive-buffer 100000
ACOS(config-quic)# burst-len 30
ACOS(config-quic)# key-update-to-client
ACOS(config-quic)# key-update-to-server
ACOS(config-quic)# server-retry
```

Example The following commands bind the SLB template QUIC to the 'quic' virtual port:

```
ACOS(config)# slb virtual-server vip 10.10.10.10
ACOS(config-slb vserver)# port 443 quic
ACOS(config-slb vserver-vport)# source-nat pool p1
ACOS(config-slb vserver-vport)# template quic quic_http3
ACOS(config-slb vserver-vport)# template client-ssl ct
ACOS(config-slb vserver-vport)# template server-ssl st
```

Related Commands:

- port
- template quic

slb template reqmod-icap

Description Creates a template that you can apply to ACOS virtual servers to enable ICAP REQMOD message capability on the virtual server.

Syntax

```
[no] slb template reqmod-icap reqmod-template-name
```

This command changes the configuration mode to a new sub-level.

Default ACOS does not have a default SLB REQMOD ICAP template.

Mode Global Configuration mode

Usage See the "ICAP Services" section of the *SSL Insight Configuration Guide* for an overview of ICAP and usage guidelines.

Example The following example creates a REQMOD ICAP template with the name REQMOD_abcd, and then binds it to the HTTP vPort of a wildcard SLB virtual server.

```
ACOS(config)# slb server ICAP_server_1 10.1.260.11
ACOS(config-real server)# port 1344 tcp
ACOS(config-real server-node port)# health-check-disable
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group SG_ICAP tcp
ACOS(config-slb svc group)# member ICAP_server_1 1344
ACOS(config-slb svc group-member:1344)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb template reqmod-icap REQMOD_abcd
ACOS(config-reqmod-icap)# service-group SG_ICAP
ACOS(config-reqmod-icap)# service-url icap://abcd.com/reqmod_
abcd
ACOS(config-reqmod-icap)# exit
ACOS(config)# slb virtual-server wildcard_VIP 0.0.0.0 acl 100
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template reqmod-icap REQMOD_
abcd
```

allowed-http-methods

Description List of allowed HTTP methods.

Syntax

```
[no] allowed-http-methods methods
```

The allowed methods that can be specified are GET, POST, HEAD, PUT, OPTIONS, TRACE, DELETE, PURGE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK.

Default If no methods are specified, the default is to allow all HTTP methods.

Mode SLB REQMOD ICAP template

Usage See RFC 3507 for further information on methods.

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# allowed-http-methods GET

ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# allowed-http-methods "MKCOL GET"
ACOS(config-reqmod-icap)# show config slb template reqmod-icap
Reqmod_Template
!Section configuration: 80 bytes
!
slb template reqmod-icap Reqmod_Template
  allowed-http-methods "MKCOL GET"
!
```

Example Use the **no** form of the command to return to the default where all HTTP methods are allowed. The following example removes the restrictions of the previous example that allowed only MKCOL and GET, and returns to the default where all HTTP methods are allowed::

```
ACOS(config-reqmod-icap)# no allowed-http-methods "MKCOL GET"
ACOS(config-reqmod-icap)# show config slb template reqmod-icap
Reqmod_Template
!Section configuration: 80 bytes
!
slb template reqmod-icap Reqmod_Template
!
```

Example If ACOS does not recognize or allow the methods you enter in the command, you will get the following error message listing the all allowed methods:

```
ACOS(config-reqmod-icap)# allowed-http-methods ALL
Unsupported HTTP method in list, Supported methods are: GET
POST HEAD PUT OPTIONS TRACE DELETE PURGE PROPFIND PROPPATCH
MKCOL COPY MOVE LOCK UNLOCK
```

disable-http-server-reset

Description Prevents the HTTP server from resetting.

Syntax

```
[no] disable-http-server-reset
```

Default Enabled

Mode SLB REQMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# disable-http-server-reset
```

fail-close

Description Mark the virtual port down when the template service group is down.

Syntax

```
[no] fail-close
```

Default Not enabled.

Mode SLB REQMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# fail-close
```

include-protocol-in-uri

Description Include the protocol and port in the HTTP URI sent to the ICAP server.

Syntax

```
[no] include-protocol-in-uri
```

Default Not enabled.

Mode SLB REQMOD ICAP template

Usage See RFC 2396 for further information on URIs.

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# include-protocol-in-uri
```

log-only-allowed-method

Description Configures device to print ICAP logs for only HTTP requests sent to the ICAP server that are designated as "allowed" by the "allow-http-

methods" command. Logs are printed for all requests that the device forwards to ICAP or receives from ICAP.

When this option is not enabled, logs are printed for all HTTP requests sent to ICAP. By default, this option is not enabled.

Syntax `[no] log-only-allowed-method`

Default Not enabled.

Mode SLB REQMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# log-only-allowed-method
ACOS(config-reqmod-icap)#
```

min-payload-size

Description Set the minimum payload size sent to the ICAP server.

Syntax `[no] min-payload-size num`

Parameter	Description
num	Set the minimum payload size. You can specify 1-65536.

Default 4096

Mode SLB REQMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# min-payload-size 8192
```

preview

Description Specifies the number of bytes that ACOS forwards to the ICAP server at the beginning of a transaction.

If you do not configure a preview value, the ACOS device uses the preview value obtained from the ICAP server.

Syntax

```
[no] preview num
```

Parameter	Description
num	The number of bytes that ACOS forwards to the ICAP server at the beginning of a transaction. This number applies only to the encapsulated body (the HTTP payload).

Default 32768

Mode SLB REQMOD ICAP template

Usage If you enter the default value of the command or use the `no` form of the command to remove the setting (`no preview num`), ACOS uses the preview value obtained from the ICAP server. See RFC 3507 for further information.

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# preview 8192
```

service-group

Description Specify the names of the ICAP service groups.

Syntax

```
[no] service-group service-group-name
```

Parameter	Description
service-group-name	Name of a configured service-group.

Mode SLB REQMOD ICAP and SLB RESPMOD ICAP templates

Example Example configuration for REQMOD ICAP:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# service-group SSLi_SG1
```

Example Example configuration for RESPMOD ICAP:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# service-group SSLi_SG1
```

service-url

Description Specify the URLs of the ICAP servers.

Syntax

```
[no] service-url url
```

Parameter	Description
url	URL to send to the ICAP servers.

Mode SLB REQMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# service-url icap://ExampleURL.com
```

template

Description Apply an ACOS template to this ICAP template.

Syntax

```
[no] template type name
```

Parameter	Description
type	The following templates can be applied: • **logging**—apply the specified logging template. See the `slb template logging` command for information on configuring a logging template. Web logging is described in detail in the "Web Logging for HTTP and RAM Caching" section of the Application Delivery Controller Guide. • **server-ssl**—apply the specified server-SSL template. Enables a secure SSL connection to the ICAP server. • **tcp-proxy**—apply the specified TCP proxy template.
name	Name of the desired template.

Mode SLB REQMOD and RESPMOD ICAP template

Example Apply a logging template to REQMOD ICAP template:

```
ACOS(config)# slb template reqmod-icap Reqmod_Template
ACOS(config-reqmod-icap)# template logging SSLi_Logging_
Template
```

Example Apply a logging template to RESPMOD ICAP template:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# template logging SSLi_Logging_
Template
```

slb template respmod-icap

Description Creates a template that you can apply to ACOS virtual servers to enable ICAP RESPMOD message capability on the virtual server.

Syntax

```
[no] slb template respmod-icap respmod-template-name
```

Default ACOS does not have a default SLB RESPMOD ICAP template.

Mode Global Configuration mode

Usage See the “Redirection of SSLi Sessions to ICAP Servers” section of the *SSL Insight Configuration Guide* for an overview of ICAP and usage guidelines.

Example The following example creates a RESPMOD ICAP template with the name RESPMOD_abcd, and then binds it to the HTTP vPort of a wildcard SLB virtual server.

```
ACOS(config)# slb server ICAP_server_1 10.1.260.11
ACOS(config-real server)# port 1344 tcp
ACOS(config-real server-node port)# health-check-disable
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group SG_ICAP tcp
ACOS(config-slb svc group)# member ICAP_server_1 1344
ACOS(config-slb svc group-member:1344)# exit
ACOS(config-slb svc group)# exit
```

```
ACOS(config)# slb template respmod-icap RESPMOD_abcd
ACOS(config-reqmod-icap)# service-group SG_ICAP
ACOS(config-reqmod-icap)# service-url icap://abcd.com/respmod_
abcd
ACOS(config-reqmod-icap)# exit
ACOS(config)# slb virtual-server wildcard_VIP 0.0.0.0 acl 100
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template respmod-icap RESPMOD_
abcd
```

disable-http-server-reset

Description Prevents the HTTP server from resetting.

Syntax

```
[no] disable-http-server-reset
```

Default Enabled

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# disable-http-server-reset
```

fail-close

Description Mark the virtual port down when the template service group is down.

Syntax

```
[no] fail-close
```

Default Not enabled.

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# fail-close
```

include-protocol-in-uri

Description Include the protocol and port in the HTTP URI sent to the ICAP server.

Syntax `[no] include-protocol-in-uri`

Default Not enabled.

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# include-protocol-in-uri
```

log-only-allowed-method

Description Configures device to print ICAP logs for only HTTP requests sent to the ICAP server that are designated as "allowed" by the "allow-http-methods" command. Logs are printed for all requests that the device forwards to ICAP or receives from ICAP.

When this option is not enabled, logs are printed for all HTTP requests sent to ICAP. By default, this option is not enabled.

Syntax `[no] log-only-allowed-method`

Default Not enabled.

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# log-only-allowed-method
ACOS(config-respmod-icap)#
```

min-payload-size

Description Set the minimum payload size.

Syntax `[no] min-payload-size num`

Parameter	Description
num	Set the minimum payload size. You can specify 1-65536.

Default 4096

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# min-payload-size 8192
```

preview

Description Command to allow the ICAP server to preview to RESPMOD messages.

If you do not configure a preview value, the ACOS device uses the preview value obtained from the ICAP server.

Syntax

```
[no] preview num
```

Parameter	Description
num	The number of bytes the ACOS device forwards to the ICAP server at the beginning of a transaction. This number applies only to the encapsulated body (the HTTP payload).

Default 32768

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# preview 8192
```

service-group

Description Specify the names of the ICAP service groups.

Syntax

```
[no] service-group service-group-name
```

Parameter	Description
service-group-name	Name of a configured service-group.

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# service-group SSLi_SG1
```

service-url

Description Specify the URLs of the ICAP servers.

Syntax

```
[no] service-url url
```

Parameter	Description
url	URL to send to the ICAP servers.

Mode SLB RESPMOD ICAP template

Example Example configuration:

```
ACOS(config)# slb template respmod-icap Respmod_Template
ACOS(config-respmod-icap)# service-url icap://ExampleURL.com
```

template

Description Apply an ACOS template to this ICAP template.

Syntax

```
[no] template type name
```

Parameter	Description
type	The following templates can be applied: • **logging**—apply the specified logging template. See the `slb template logging` command for information on configuring a logging template. Web logging is described in detail in the "Web Logging for HTTP and RAM Caching" section of the *Application Delivery* **Controller** *Guide*. • **server-ssl**—apply the specified server-SSL template. Enables a secure SSL connection to the ICAP server.

Parameter	Description
	• **tcp-proxy**—apply the specified TCP proxy template.
name	Name of the desired template.

Mode SLB RESPMOD ICAP template

slb template server

Description Configure a template of SLB settings for real servers.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all real ports that use the template.

Syntax

```
[no] slb template server {default | template-name}
```

Parameter	Description
default	Edit the default real server template. This template can be modified in the same way as any custom *template-name* you specify.
template-name	Template name (1-127 characters)

Mode Configuration mode

Usage The normal form of this command creates a real server template. The **no** form of this command removes the template.

You can bind only one real server template to a real server. However, you can bind the real server template to multiple real servers.

Some of the parameters that can be set using a template can also be set or changed on the individual server.

- If a parameter is set (or changed from its default) in both a template and on the individual server, the setting on the individual server takes precedence.

- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual server, the setting in the template takes precedence.

Example The following commands configure a real server template called “rs-tmplt1” and bind the template to two real servers:

```
ACOS(config)# slb template server rs-tmplt1
ACOS(config-rserver)# health-check ping2
ACOS(config-rserver)# conn-limit 500000
ACOS(config-rserver)# exit
ACOS(config)# slb server rs1 10.1.1.99
ACOS(config-real server)# template server rs-tmplt1
ACOS(config-real server)# exit
ACOS(config)# slb server rs2 10.1.1.100
ACOS(config-real server)# template server rs-tmplt1
```

Example The following commands configure hostname server parameters in a server port template and a server template:

```
ACOS(config)# slb template port temp-port
ACOS(config-rport)# dynamic-member-priority 12
ACOS(config-rport)# exit
ACOS(config)# slb template server temp-server
ACOS(config-rserver)# dns-query-interval 5
ACOS(config-rserver)# min-ttl-ratio 3
ACOS(config-rserver)# max-dynamic-server 16
ACOS(config-rserver)# exit
```

bw-rate-limit

Description Configure the bandwidth rate limit for servers that use this template.

Syntax

```
[no] bw-rate-limit l-num resume r-num duration d-num [no-logging]
```

Parameter	Description
l-num	Bandwidth rate limit number in Kbps (1-16777216).
r-num	Resume port selection after bandwidth drops below this threshold, in Kbps (1-16777216).

Parameter	Description
d-num	Time period the rate limit needs to honor to both exceed bw-rate-limit number and drop below resume number, in seconds (1-250).
no-logging	Do not log bandwidth rate limit related state transitions.

Default Not set

Mode SLB server template

bw-rate-limit-acct

Description Configure the bandwidth rate limit accounting for servers that use this template.

Syntax

```
[no] bw-rate-limit-acct TRAFFIC
```

Parameter	Description
TRAFFIC	Specifies data limited by command. Options include: • to-server-only – Account for traffic sent to the real server. • from-server-only – Account for traffic received from the real server. • all – Account for all traffic sent to/received from real server (default).

Default Not set

Mode SLB server template

conn-limit

Description Maximum number of connections allowed on real servers using this template.

Syntax

```
[no] conn-limit max-num [resume resume-num] [no-logging]
```

Parameter	Description
max-num	Maximum number of concurrent connections (1-64000000).
resume-num	Maximum number of connections the server can have before the ACOS device resumes use of the server (1-1048575).
no-logging	Disables logging for this feature.

Default 64000000 (64 million)

Mode SLB server template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure 7 million as the maximum number of connections, with no logging:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# conn-limit 7000000 no-logging
```

conn-rate-limit

Description Limits the rate of new connections the ACOS device is allowed to send to servers that use this template. When a real server reaches its connection limit, the ACOS device stops selecting the server for client requests.

Syntax

```
[no] conn-rate-limit connections [per {100ms | 1sec}] [no-logging]
```

Parameter	Description
connections	Maximum number of new connections allowed on

Parameter	Description
	a server. You can specify 1-1048575 connections.
per {**100ms** | **1sec**}	Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (1sec).
no-logging	Disable logging when this feature is enabled.

Default By default this is not set; when enabled, the default sampling rate is per 1sec.

Mode SLB server template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure 1 million as the maximum number of new connections per second, with no logging:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# conn-rate-limit 1000000 per 1sec no-logging
```

dns-query-interval

Description Specifies how often the ACOS device sends DNS queries for the IP addresses of dynamic real servers.

Syntax

```
[no] dns-query-interval minutes
```

Parameter	Description
minutes	DNS query interval in minutes (1-1440 minutes, or one day).

Default 10 minutes

Mode SLB server template

Example Configure 30 minutes as the DNS query interval:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# dns-query-interval 30
```

dynamic-server-prefix

Description Specifies the prefix added to the front of dynamically created servers.

Syntax

```
[no] dynamic-server-prefix string
```

Parameter	Description
string	Prefix string (1-3 characters).

Default The default string is “DRS”

Mode SLB server template

Example Configure “MDS” as the server prefix string:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# dynamic-server-prefix MDS
```

extended-stats

Description Enables collection of peak connection statistics for a server.

Syntax

```
[no] extended-stats
```

Default Disabled by default

Mode SLB server template

Example Enable the feature:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# extended-stats
```

health-check

Description Enables health monitoring of ports that use this template.

Syntax `[no] health-check [name]`

Parameter	Description
name	Name of a configured health monitor.

Mode SLB server template

Usage If this command is not used, or is used without a specific monitor *name*, the default ICMP health monitor is used; a ping is sent every 30 seconds. If the ping fails 2 times consecutively, the ACOS device sets the server state to DOWN.

Example Use the health monitor named “hm1”:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# health-check hm1
```

health-check-disable

Description Disables health monitoring of servers that use this template.

Syntax `[no] health-check-disable`

Mode SLB server template

Example Disable server health monitoring:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# health-check-disable
```

l2-health-check-path

Description Configure the layer 2 health check path to indicate that the server state needs to be synchronized with the system path object.

The system path object (system path command) is defined under Global configuration mode . For more information, refer *Command Line Reference*.

Syntax `[no] l2-health-check-path <system_path_object_name>`

Default Disabled

Mode Real server

Usage This option or feature is supported for interface real server only.

The path object will inform the associated interface server when its state changes. The real server synchronizes its state according to the received event. It also queries the path's state every second to ensure that its state is synchronized with the path.

Once this option is removed from the interface server, the system maintains the server state using the default method of synchronizing the state with the attached interface.

Example The following commands configure an interface server for layer 2 health check:

```
ACOS(config)# slb server S1 ethernet 3
ACOS(config-real server)# l2-health-check-path test_path
ACOS(config-real server)# port 80 tcp
```

log-selection-failure

Description Enables real-time logging for server-selection failures.

Syntax

```
[no] log-selection-failure
```

Default Disabled by default.

Mode SLB server template

Example Enable the logging of server-selection failures:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# log-selection-failure
```

max-dynamic-server

Description Maximum number of dynamic real servers that can be created for a given hostname.

Syntax

```
[no] max-dymanic-server [num]
```

Parameter	Description
num	Maximum number of servers (1-1023).

Default 255

Mode SLB server template

Example Allow a maximum of 500 dynamic real servers to be created:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# max-dynamic-server 500
```

min-ttl-ratio

Description Minimum initial value for the TTL of dynamic real servers. The ACOS device multiplies this value by the DNS query interval to calculate the minimum TTL value to assign to the dynamically created server.

Syntax

```
[no] min-ttl-ratio [num]
```

Parameter	Description
num	Initial value (1-15).

Default 2

Mode SLB server template

Example Configure a DNS query interval of 30 minutes and minimum initial value of 3; this will set the TTL of dynamic real servers to 90:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# dns-query-interval 30
ACOS(config-rserver)# min-ttl-ratio 3
```

slow-start

Description Provides time for real ports that use the template to ramp-up after TCP/UDP service is enabled, by temporarily limiting the number of new connections on the ports.

Syntax

```
[no] slow-start
[from starting-conn-limit]
[times scale-factor | add conn-incr]
```

```
[every interval]
[till ending-conn-limit]
```

Parameter	Description
starting-con-limit	Maximum number of concurrent connections to allow on the server after it first comes up. You can specify from 1-4095 concurrent connections. The default is 128.
scale-factor	Number by which to multiply the starting connection limit. For example, if the scale factor is 2 and the starting connection limit is 128, the ACOS device increases the connection limit to 256 after the first ramp-up interval. The scale factor can be 2-10. The default is 2.
conn-incr	As an alternative to specifying a scale factor, you can instead specify how many more concurrent connections to allow. You can specify 1-4095 new connections.
interval	Number of seconds between each increase of the number of concurrent connections allowed. For example, if the ramp-up interval is 10 seconds, the number of concurrent connections to allow is increased every 10 seconds. The ramp-up interval can be 1-60 seconds. The default is 10 seconds.
ending-conn-limit	Maximum number of concurrent connections to allow during the final ramp-up interval. After the final ramp-up interval, the slow start is over and does not limit further connections to the server. You can specify from 1-65535 connections. The default is 4096.

Default Slow-start is disabled by default.

Mode SLB server template

Usage If a normal runtime connection limit is also configured on the server (for example, by the conn-limit command), and the normal connection limit is smaller than the slow-start ending connection limit, the ACOS device limits slow-start connections to the maximum allowed by the normal connection limit.

Example Enable slow-start using the default values:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# slow-start
```

spoofing-cache

Description Enables support for a spoofing cache server. A spoofing cache server uses the client's IP address instead of its own as the source address when obtaining content requested by the client.

Syntax

```
[no] spoofing-cache
```

Default Disabled.

Mode SLB server template

Example Enable this feature:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# spoofing-cache
```

stats-data-disable

Description Disable statistical data collection for servers that use this template.

Syntax

```
stats-data-disable
```

Default Statistical data collection is enabled by default.

Mode SLB server template

Example Disable stats data collection:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# stats-data-disable
```

stats-data-enable

Description Enable statistical data collection for servers that use this template.

Syntax

```
stats-data-enable
```

Default Statistical data collection is enabled by default.

Mode SLB server template

Example Enable stats data collection:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# stats-data-enable
```

support-http2

Description Start the HTTP/2 connection with prior knowledge and send HTTP/2 frames directly.

Syntax

```
[no] support-http2 {only}
```

Parameter	Description
support-http2	Specify this command in a real server if the server side supports HTTP/2. ACOS will send the HTTP/2 request with prior-knowledge to the server if the client request is HTTP/2. **NOTE:** The HTTP/1.1 to HTTP/2 upgrade mechanism will not be supported as specified in RFC 9113.
only	This is an optional parameter. Specify this option when the server side can only handle HTTP/2 traffic. This option should be enabled only when the HTTP/2 is configured on the server side. For more information, see HTTP/1.1 to HTTP/2 communication support section in *Application Delivery Controller Guide*.

Default Not enabled.

Mode SLB real server

Example The following command enables HTTP/2 support on real server.

```
ACOS(config)# slb server realserver1 10.1.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# support-http2
```

Related Commands:

- slb template http

weight

Description Assigns an administrative weight to the server, for weighted load balancing.

Syntax

```
[no] weight num
```

Parameter	Description
num	Administrative weight assigned to the server. You can specify 1-1000.

Default 1

Mode SLB server template

Example Assign an administrative weight of 5:

```
ACOS(config)# slb template server default
ACOS(config-rserver)# weight 5
```

slb template sip (over TCP/TLS)

Description Configure separate load balancing of Session Initiation Protocol (SIP) registration traffic and non-registration traffic for SIP over TCP/TLS.

Syntax

```
[no] slb template sip template-name
```

Parameter	Description
template-name	Template name (1-127 characters)

This command enters the specified SIP (over UDP) template.

Default The configuration does not have a default SIP over TCP/TLS template.

Mode Configuration mode

Usage The normal form of this command creates a SIP configuration template. The **no** form of this command removes the template.

You can bind only one SIP template to a virtual port. However, you can bind the same SIP template to multiple ports.

Example The following commands configure a SIP over TCP/TLS template:

```
ACOS(config)# slb template sip siptls-tmplt
ACOS(config-sip)# insert-client-ip
ACOS(config-sip)#  client-keep-alive
ACOS(config-sip)#  failed-client-selection "480 Temporarily
Unavailable"
ACOS(config-sip)#  failed-server-selection "504 Server Time-
out"
ACOS(config-sip)#  exclude-translation header Authentication
```

alg-dest-nat

Description Enables SIP ALG support for the destination IP address.

Syntax

```
[no] alg-dest-nat
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# alg-dest-nat
```

alg-source-nat

Description Enables SIP ALG support for the source IP address.

ALG support status does not affect IP layer address translation. IP layer address translation is still performed, if applicable, even when ALG support is disabled.

Syntax

```
[no] alg-source-nat
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# alg-source-nat
```

call-id-persist-disable

Description Disables call-ID persistence.

Syntax

```
[no] call-id-persist-disable
```

Default Call-ID persistence is enabled by default.

Mode SLB SIP template

Example Disable call-ID persistence.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# call-id-persist-disable
```

client-keepalive

Description Enables the ACOS device to respond to SIP pings from clients on behalf of SIP servers. When this option is enabled, the ACOS device responds to a SIP ping from a client with a “pong”. This option is disabled by default.

If connection reuse is configured, even if client keepalive is disabled, the ACOS device will respond to a client SIP ping with a pong.

Syntax

```
[no] client-keepalive
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-keepalive
```

client-request-header erase

Description Erases the specified header.

Syntax

```
[no] client-request-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-request-header erase Max-Forwards
```

client-request-header insert

Description Inserts the specified header into requests.

Syntax

```
[no] client-request-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description
field *:value*	Header field name and the value to insert. Use a colon between the header name and the value. To use a blank space between the header name and

Parameter	Description

	the value, use double quotation marks.
	Examples:
	`client-request-header insert Max-Forwards:15`
	`client-request-header insert "Max-Forwards: 15"`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a request already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the "Max-Forwards: 15" header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-request-header insert "Max-Forwards: 15"
```

client-response-header erase

Description Erases the specified header.

Syntax

```
[no] client-response-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-response-header erase Max-Forwards
```

client-response-header insert

Description Inserts the specified header into responses.

Syntax

```
[no] client-response-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description

field *:value*	Header field name and the value to insert.
	
	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	
	Examples:
	
	`client-response-header insert Max-Forwards:15`
	
	`client-response-header insert “Max-Forwards: 15”`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a response already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the “Max-Forwards: 15” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-response-header insert “Max-Forwards:
15”
```

dialog-aware

Description Enables multiple active client instance support with the same end-user login.

Syntax

```
[no] dialog-aware
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# dialog-aware
```

exclude-translation

Description Disables translation of the virtual IP address and virtual port in specific portions of SIP messages.

Syntax

```
[no] exclude-translation {body | header string | start-line}
```

Parameter	Description
body	Does not translate virtual IP addresses and virtual ports in the body of the message.
string	Does not translate virtual IP addresses and virtual ports in the specified header.
start-line	Does not translate virtual IP addresses and virtual ports in the SIP request line or status line.

Default Not set; the ACOS device does not translate addresses in any header except the top Via header.

Mode SLB SIP template

Example Do not translate virtual IP addresses and virtual ports in the message body:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# exclude-translation body
```

failed-client-selection

Description Specifies the response when selection of an SIP client fails.

This option is applicable only if the configuration includes a connection-reuse template.

Syntax

```
[no] failed-client-selection {string | drop}
```

Parameter	Description
string	Message string to send to the server; for example: "480 Temporarily Unavailable" If the message string contains a space, use double quotation marks around the string.
drop	Drop the traffic.

Default Not set; the ACOS device resets the connection when selecting an SIP server fails

Mode SLB SIP template

Example Configure a response for failed client selection:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# failed-client-selection "480 Temporarily
Unavailable"
```

failed-server-selection

Description Specifies the response when selection of an SIP server fails.

Syntax

```
[no] failed-server-selection {string | drop}
```

Parameter	Description
string	Message string to send to the client; for example: "504 Server Time-Out" If the message string contains a space, use double quotation marks around the string.
drop	Drop the traffic.

Default Not set; the ACOS device resets the connection when selection of an SIP server fails

Mode SLB SIP template

Example Configure a response for failed server selection:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# failed-server-selection "504 Server Time-Out"
```

insert-client-ip

Description Inserts an "X-Forwarded-For: IP-address:port" header into SIP packets from the client to the SIP server. The header contains the client IP address and source protocol port number. The ACOS device uses the header to identify the client when forwarding a server reply.

Syntax

```
[no] insert-client-ip
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# insert-client-ip
```

server-keep-alive

Description For configurations that use a connection-reuse template, this option specifies how often the ACOS device sends a SIP ping on each persistent connection. The ACOS device silently drops the server's reply. If the server does not reply to a SIP ping within the connection-reuse timeout, the ACOS device closes the persistent connection.

The connection-reuse timeout is configured by the timeout command at the configuration level for the slb template connection-reuse.

Syntax

```
[no] server-keep-alive num
```

Parameter	Description
num	Number of seconds (5-300).

Mode SLB SIP template

Example Configure the keep-alive for 10 seconds:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-keep-alive 10
```

server-request-header erase

Description Erases the specified header.

Syntax

```
[no] server-request-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-request-header erase Max-Forwards
```

server-request-header insert

Description Inserts the specified header into requests.

Syntax

```
[no] client-request-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description
field *:value*	Header field name and the value to insert.

Parameter	Description

	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	Examples:
	`server-request-header insert Max-Forwards:15`
	`server-request-header insert "Max-Forwards: 15"`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a request already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the "Max-Forwards: 15" header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-request-header insert "Max-Forwards: 15"
```

server-response-header erase

Description Erases the specified header.

Syntax

```
[no] server-response-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-response-header erase Max-Forwards
```

server-response-header insert

Description Inserts the specified header into responses.

Syntax

```
[no] server-response-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description

field *:value*	Header field name and the value to insert.
	
	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	
	Examples:
	
	`client-response-header insert Max-Forwards:15`
	
	`client-response-header insert “Max-Forwards: 15”`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a response already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the “Max-Forwards: 15” header:

```
ACOS(config)# slb template sip sip-tmp1
```

```
ACOS(config-sip)# server-response-header insert "Max-Forwards: 15"
```

server-selection-per-request

Description Forces the ACOS device to perform the server selection process anew for every SIP request. Without this option, the ACOS device reselects the same server for subsequent requests (assuming the same server group is used), unless overridden by other template options. This option applies to SIP-TCP and SIPS virtual ports. The option is unnecessary for SIP over UDP. Strict transaction switching is automatically used for SIP over UDP.

Syntax

```
[no] server-selection-per-request
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-selection-per-request
```

smp-call-id-rtp-session

Description Create a cross-CPU call-ID RTP session.

This feature enables your ACOS device to monitor RTP and SIP traffic. This command creates a cross-CPU RTP session which can be matched by RTP traffic.

Use this command with rtp-sip-call-id-match to configure this feature.

Syntax

```
[no] smp-call-id-rtp-session
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
!
slb template sip test
```

```
   smp-call-id-rtp-session
!
!
slb virtual-server vv 0.0.0.0
   port 0 udp
      skip-rev-hash
      message-switching
      force-routing-mode
      no-dest-nat
      service-group win
     rtp-sip-call-id-match
   port 5060 sip
      message-switching
      force-routing-mode
      service-group winms
      template sip test
!
```

timeout

Description Specifies the number of minutes a SIP session can remain idle before the ACOS device terminates the session.

Syntax

```
[no] timeout num
```

Parameter	Description
num	Number of minutes (1-250).

Default 30 minutes

Mode SLB SIP template

Example Configure the timeout for 5 minutes:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# timeout 5
```

slb template sip (over UDP)

Description Configure separate load balancing of Session Initiation Protocol (SIP) registration traffic and non-registration traffic for SIP clients.

Syntax

```
[no] slb template sip template-name
```

Parameter	Description
template-name	Template name (1-127 characters)

This command enters the specified SIP (over UDP) template.

Default The configuration does not have a default SIP over UDP template.

Mode Configuration mode

Usage The normal form of this command creates a SIP configuration template. The **no** form of this command removes the template.

You can bind only one SIP template to a virtual port. However, you can bind the same SIP template to multiple ports.

The **header-erase** and **header-insert** options apply to both traffic directions, client-to-server and server-to-client traffic.

Example The following commands configure a SIP template named “Registrar_ template”:

```
ACOS(config)# slb template sip Registrar_template
ACOS(config-sip)# registrar service-group Registrar_gp
ACOS(config-sip)# client-request-header insert max-Forwards:15
ACOS(config-sip)# client-request-header erase Contact
```

alg-dest-nat

Description Translates the VIP address into the real server IP address in SIP messages, when destination NAT is used.

Syntax

```
[no] alg-dest-nat
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# alg-dest-nat
```

alg-source-nat

Description Translates source IP address in to the NAT IP address in SIP messages, when source NAT is used.

ALG support status does not affect IP layer address translation. IP layer address translation is still performed, if applicable, even when ALG support is disabled.

Syntax

```
[no] alg-source-nat
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# alg-source-nat
```

call-id-persist-disable

Description Disables call-ID persistence.

Syntax

```
[no] call-id-persist-disable
```

Default Call-ID persistence is enabled by default.

Mode SLB SIP template

Example Disable call-ID persistence.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# call-id-persist-disable
```

client-request-header erase

Description Erases the specified header.

Syntax

```
[no] client-request-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-request-header erase Max-Forwards
```

client-request-header insert

Description Inserts the specified header into requests.

Syntax

```
[no] client-request-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description

field *:value*	Header field name and the value to insert.
	
	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	
	Examples:
	
	`client-request-header insert Max-Forwards:15`
	
	`client-request-header insert “Max-Forwards: 15”`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a request already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the “Max-Forwards: 15” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-request-header insert “Max-Forwards: 15”
```

client-response-header erase

Description Erases the specified header.

Syntax

```
[no] client-response-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-response-header erase Max-Forwards
```

client-response-header insert

Description Inserts the specified header into responses.

Syntax

```
[no] client-response-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description
field	Header field name and the value to insert.

Parameter	Description

:value	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	Examples:
	`client-response-header insert Max-Forwards:15`
	`client-response-header insert "Max-Forwards: 15"`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a response already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the "Max-Forwards: 15" header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# client-response-header insert "Max-Forwards: 15"
```

dialog-aware

Description Enables multiple active client instance support with the same end-user login.

Syntax

```
[no] dialog-aware
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
```

```
ACOS(config-sip)# dialog-aware
```

exclude-translation

Description Disables translation of the virtual IP address and virtual port in specific portions of SIP messages.

Syntax

```
[no] exclude-translation {body | header string | start-line}
```

Parameter	Description
body	Does not translate virtual IP addresses and virtual ports in the body of the message.
string	Does not translate virtual IP addresses and virtual ports in the specified header.
start-line	Does not translate virtual IP addresses and virtual ports in the SIP request line or status line.

Default Not set; the ACOS device does not translate addresses in any header except the top Via header.

Mode SLB SIP template

Example Do not translate virtual IP addresses and virtual ports in the message body:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# exclude-translation body
```

insert-client-ip

Description Inserts an “X-Forwarded-For: IP-address:port” header into SIP packets from the client to the SIP server. The header contains the client IP address and source protocol port number. The ACOS device uses the header to identify the client when forwarding a server reply.

Syntax

```
[no] insert-client-ip
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# insert-client-ip
```

keep-server-ip-if-match-acl

Description Disables reverse NAT based on the IP addresses in an extended ACL. This command is useful in cases where a SIP server needs to reach another server, and the traffic must pass through the ACOS device.

Syntax

```
[no] keep-server-ip-if-match-acl
```

Default Not enabled.

Mode SLB SIP template

Example Enable this feature.

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# keep-server-ip-if-match-acl
```

registrar service-group

Description Specifies the name of a service group of SIP Registrar servers.

Syntax

```
[no] registrar service-group name
```

Parameter	Description
name	Service group name (1-127 characters).

Mode SLB SIP template

Example Specify “sip-sg1” as the service group:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# registrar service-group sip-sg1
```

server-request-header erase

Description Erases the specified header.

Syntax

```
[no] server-request-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-request-header erase Max-Forwards
```

server-request-header insert

Description Inserts the specified header into requests.

Syntax

```
[no] client-request-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description

field *:value*	Header field name and the value to insert.
	
	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	
	Examples:
	
	`server-request-header insert Max-Forwards:15`
	
	`server-request-header insert “Max-Forwards: 15”`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a request already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the “Max-Forwards: 15” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-request-header insert “Max-Forwards: 15”
```

server-response-header erase

Description Erases the specified header.

Syntax

```
[no] server-response-header erase string [all]
```

Parameter	Description
string	Specify the header to erase.
all	Erase all instances of the specified header. If not specified, only the first instance is erased.

Default All instances of the specified header are erased.

Mode SLB SIP template

Example Erase the first instance of the “Max-Forwards” header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-response-header erase Max-Forwards
```

server-response-header insert

Description Inserts the specified header into responses.

Syntax

```
[no] server-response-header insert field:value
[insert-always | insert-if-not-exist]
```

Parameter	Description
field	Header field name and the value to insert.

Parameter	Description

:value	Use a colon between the header name and the value. To use a blank space between the header name and the value, use double quotation marks.
	Examples:
	`client-response-header insert Max-Forwards:15`
	`client-response-header insert "Max-Forwards: 15"`

insert-always	Always inserts the *field*:*value* pair. If the request already contains a header with the same field name, the new *field*:*value* pair is added after the existing *field*:*value* pair. Existing headers are not replaced.
insert-if-not-exist	Inserts the header only if the request does not already contain a header with the same field name.

Without either **insert-always** or **insert-if-not-exist** option, if a response already contains one or more headers with the specified field name, the command replaces the last header.

Mode SLB SIP template

Example Insert the "Max-Forwards: 15" header:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# server-response-header insert "Max-Forwards: 15"
```

timeout

Description Specifies the number of minutes a SIP session can remain idle before the ACOS device terminates the session.

Syntax

```
[no] timeout num
```

Parameter	Description
num	Number of minutes (1-250).

Default 30 minutes

Mode SLB SIP template

Example Configure the timeout for 5 minutes:

```
ACOS(config)# slb template sip sip-tmp1
ACOS(config-sip)# timeout 5
```

slb template smpp

Description Configure SMPP 3.3 protocol load balancing template.

Syntax `[no] slb template smpp template-name`

Parameter	Description
template-name	Template name (1-127 characters)

This command enters the specified SMPP template.

Default The configuration does not have a default SMPP template.

Usage The normal form of this command creates an SMPP template. The **no** form of this command removes the template.

Mode Configuration mode

client-enquire-link

Description When enabled, ACOS replies to clients directly with an ENQUIRE_LINK message. The ENQUIRE_LINK message prevents the client connection from timing out and serves the same purpose as a keepalive message.

Syntax `[no] client-enquire-link`

Default Not enabled.

Mode SLB SMPP template

Example Enable this feature.

```
ACOS(config)# slb template smpp smpp-tmp1
ACOS(config-smpp)# client-enquire-link
```

server-enquire-link

Description Prevents reusable connections to the SMPP server from aging out. When this option is enabled, ACOS regularly sends an ENQUIRE_LINK message to the SMPP server to maintain the client-to-server connection.

Syntax

```
[no] server-enquire-link num
```

Parameter	Description
num	Number of seconds at which the keepalive message is sent (5-300).

Default 30 seconds.

Mode SLB SMPP template

Example Set the interval to 15 seconds.

```
ACOS(config)# slb template smpp smpp-tmp1
ACOS(config-smpp)# server-enquire-link 15
```

server-selection-per-request

Description Forces ACOS to perform server selection process for each SMPP request. Without this option, ACOS device selects same server for subsequent requests, assuming same server group is used, unless overridden by other template options.

This command works only in conjunction with a connection-reuse template. In addition, this command requires that a username-password pair is configured in the SMPP template, so that ACOS can immediately authenticate SMPP clients for every instance of server selection.

Syntax

```
[no] server-selection-per-request
```

Default Not enabled.

Mode SLB SMPP template

Example Enable this feature and configure a username-password pair.

```
ACOS(config)# slb template smpp smpp-tmp1
ACOS(config-smpp)# server-selection-per-request
ACOS(config-smpp)# user exampleuser password examplepassword
```

user

Description Sets a username and password which the ACOS device uses to authenticate SMPP clients.

If you configure a user and password, you must configure the same username-password pair for all SMPP clients and servers. Otherwise, the ACOS device will never open a TCP connection between the clients and servers.

Syntax

```
[no] user username password password
```

Parameter	Description
username	User name to use for SMPP client authentication (1-63 characters).
password	Password to use for SMPP client authentication (1-63 characters).

Mode SLB SMPP template

Example Create “exampleuser” and “examplepassword”.

```
ACOS(config)# slb template smpp smpp-tmp1
ACOS(config-smpp)# user exampleuser password examplepassword
```

slb template smtp

Description Configure STARTTLS support for Simple Mail Transfer Protocol (SMTP) clients.

Syntax

```
[no] slb template smtp template-name
```

Parameter	Description
template-name	Template name (1-127 characters)

This command enters the specified SMTP template.

Usage

The normal form of this command creates an SMTP template. The **no** form of this command removes the template.

You can bind only one SMTP template to a virtual port. However, you can bind the same SMTP template to multiple ports.

Example

The following commands configure an SMTP template named “secure-mail”. The template enforces use of STARTTLS by mail clients, disables client use of certain SMTP commands, and directs clients to a service group based on client domain.

```
ACOS(config)# slb template smtp secure-mail
ACOS(config-smtp)# starttls enforced
ACOS(config-smtp)# command-disable expn turn vrfy
ACOS(config-smtp)# client-domain-switching contains hq
service-group smtp-sg1
ACOS(config-smtp)# client-domain-switching contains
northdakota service-group smtp-sg2
```

Example

The following commands configure an SMTP template called “smtp-domain”. The template uses client domain switching to select a service group based on the email client’s domain. Clients from any domain that starts with “smb” are sent to service group “smtp-sg1”. Clients whose domain name does not start with “smb” and whose domain name contains “company1” are sent to service group “smtp-sg2”. Clients whose domain name does not match on the starts-with or contains strings and ends with “.com” are sent to service group “smtp-sg3”.

```
ACOS(config)# slb template smtp smtp-domain
ACOS(config-smtp)# client-domain-switching starts-with smb
service-group smtp-sg1
ACOS(config-smtp)# client-domain-switching contains company1
service-group smtp-sg2
ACOS(config-smtp)# client-domain-switching ends-with .com
service-group smtp-sg3
```

client-domain-switching

Description Selects a service group based on the domain of the client. You can specify all or part of the client domain name. This command is applicable when you have multiple SMTP service groups.

Syntax

```
[no] client-domain-switching {starts-with | contains | ends-with}
string service-group name
```

Parameter	Description
starts-with	Matches only if the client's domain name starts with *string*.
contains	Matches if the *string* appears anywhere within the domain name of the client.
ends-with	Matches only if the client's domain name starts with *string*.
name	Name of the service group to use for matches.

Default Not set; all client domains match, and any service group can be used.

Mode SLB SMTP template

Usage The **starts-with**, **contains**, and **ends-with** options are always applied in the following order, regardless of the order in which the commands appear in the configuration. The service group for the first match is used.

- starts-with
- contains
- ends-with

If a template has more than one command with the same option (**starts-with**, **contains**, or **ends-with**) and a client domain matches on more than one of them, the most-specific match is always used.

If a **contains** rule and an **ends-with** rule match on exactly the same string, the **ends-with** rule is used, because it has the more specific match. Here is an example of a set of client-domain-switching rules in an SMTP template. The numbers to the right indicate the precedence of

the rules when matching on client domain name “localhost”. In this case, the last rule is the best match and will be used.

```
client-domain-switching contains localhost service-group sg-a
(4)
client-domain-switching contains local service-group sg-b
(5)
client-domain-switching ends-with host service-group sg-c
(6)
client-domain-switching ends-with localhost service-group sg-d
 (3)
client-domain-switching starts-with local service-group sg-e
(2)
client-domain-switching starts-with localhost service-group
sg-f            (1)
```

Example This example directs clients to service group “smtp-sg1” if their domain contains the string “hq”:

```
ACOS(config)# slb template smtp smtp-tmp1
ACOS(config-smtp)# client-domain-switching contains hq
service-group smtp-sg1
```

command-disable

Description Disables support of the specified SMTP commands. If a client tries to issue a disabled SMTP command, ACOS sends the following message to the client:

```
502 - Command not implemented
```

Syntax

```
[no] command-disable {expn | turn | vrfy}
```

Parameter	Description
expn	Disable SMTP EXPN commands.
turn	Disable SMTP TURN commands.
vrfy	Disable SMTP VRFY commands.

Default All are enabled

Mode SLB SMTP template

Example Disable SMTP EXPN commands:

```
ACOS(config)# slb template smtp smtp-tmp1
ACOS(config-smtp)# command-disable expn
```

server-domain

Description Specifies the Email server domain. This is the domain for which the ACOS device provides SMTP load balancing.

Syntax

```
[no] server-domain name
```

Parameter	Description
name	Name of the Email server domain (1-31 characters).

Default "mail-server-domain"

Mode SLB SMTP template

Example Set "exampledomain" as the Email server domain.

```
ACOS(config)# slb template smtp smtp-tmp1
ACOS(config-smtp)# server-domain exampledomain
```

service-ready-msg

Description Specifies the text of the SMTP service-ready message sent to clients. The complete message sent to the client is constructed as follows:

```
200 - smtp-domain service-ready-string
```

NOTE: If you do not configure **server-domain** then you may see the default message text as `250-mail-server-domain`.

Syntax

```
[no] service-ready-msg string
```

Parameter	Description
string	Service-ready message (1-127 characters).

Default "ESMTP mail service ready"

Mode SLB SMTP template

Example Set “Your ESMTP mail service is ready” as the service-ready message.

```
ACOS(config)# slb template smtp smtp-tmp1
ACOS(config-smtp)# service-ready-msg "Your ESMTP mail service is ready"
```

starttls

Description Specifies whether or not use of STARTTLS by clients is required.

Syntax

```
starttls {client | server} {optional | enforced}
```

Parameter	Description
client	Configure client-side STARTTLS.
server	Configure server-side STARTTLS.
optional	Client or server can use STARTTLS but are not required to do so.
enforced	Before any mail transactions are allowed, the client must issue the STARTTLS command to establish a secured session. If the client does not issue the STARTTLS command, ACOS sends the following message to the client: `530 - Must issue a STARTTLS command first`

Default Disabled.

Mode SLB SMTP template

Example Make STARTTLS use mandatory for the client.

```
ACOS(config)# slb template smtp smtp-tmp1
ACOS(config-smtp)# starttls client enforced
```

slb template tcp

Description Create or modify a template for configuring TCP connection settings.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all virtual ports that use the template.

Syntax

```
[no] slb template tcp {default | template-name}
```

Parameter	Description
default	Edit the default TCP template. This template can be modified in the same way as any custom *template-name* you specify.
template-name	Template name (1-127 characters)

This command enters the SLB TCP Template Configuration Mode Commands for the specified TCP template.

Mode Configuration mode

Usage The normal form of this command creates a TCP configuration template. The **no** form of this command removes the template.

You can bind only one TCP template to a virtual port. However, you can bind the same TCP template to multiple ports.

Example The following commands configure a TCP template named “test” that sets the TCP window size to 1460 bytes, and bind the template to virtual service port 22 on virtual server vs1:

```
ACOS(config)# slb template tcp test
ACOS(config-l4 tcp)# initial-window-size 1460
ACOS(config-l4 tcp)# exit
ACOS(config)# slb virtual-server vs1 1.1.1.1
ACOS(config-slb vserver)# port 22 tcp
ACOS(config-slb vserver-vport)# template tcp test
```

Example The following commands configure a TCP template that quickly terminates half-open sessions while allowing active sessions to continue.

```
ACOS(config)# slb template tcp halfopen-tcp
ACOS(config-l4 tcp)# force-delete-timeout 3 alive-if-active
ACOS(config-l4 tcp)# reset-fwd
```

```
ACOS(config-l4 tcp)# reset-rev
```

del-session-on-server-down

Description This command clears a TCP session within 2 to 3 seconds if a session server is disabled by ACOS command or the server fails an ACOS health check at the service group level.

If a one or more real servers in a service group fails the health check and this command is enabled for the session, ACOS clears the session.

Active sessions, (receiving client-side packets) are cleared within 2 to 3 seconds. Idle sessions may continue to exist for more than a minute after the command is issued.

Syntax

```
[no] del-session-on-server-down
```

Default This feature is disabled by default.

Mode SLB TCP template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp tcp-tmp1
ACOS(config-l4 tcp)# del-session-on-server-down
```

force-delete-timeout

Description Specifies the maximum number of seconds a session can remain active, and forces deletion of any session still active after the specified number of seconds.

This option is useful for small, fast transactions for which the completion time of sessions is guaranteed. When used in combination with the reset-fwd and reset-rev options, the force-delete-timeout option can help clean up user connections with RSTs instead of allowing the connections to hang.

This command can not be used with the client-SSL or server-SSL template **close-notify** option. Doing so may cause unexpected behavior

Syntax

```
[no] force-delete-timeout num [alive-if-active]
```

Parameter	Description
num	Number of seconds (1-31).
alive-if-active	Terminates half-open TCP sessions on the virtual port while allowing active sessions to continue without being terminated.

Default Not set.

Mode SLB TCP template

Example Set the timeout to 10 seconds.

```
ACOS(config)# slb template tcp tcp-tmp1
ACOS(config-l4 tcp)# force-delete-timeout 10
```

force-delete-timeout-100ms

Description Specifies the maximum time (milliseconds) a session can remain active. Forces deletion of any session still active after the specified number of milliseconds.

Syntax

```
[no] force-delete-timeout-100ms num [alive-if-active]
```

Parameter	Description
num	Number of 100ms units (1-31).
alive-if-active	Terminates half-open TCP sessions on virtual port while allowing active sessions to continue without being terminated.

Default Not set.

Mode SLB TCP template

Example Set the timeout to 10 100-milliseconds (1 second).

```
ACOS(config)# slb template tcp tcp-tmp1
ACOS(config-l4 tcp)# force-delete-timeout-100ms 10
```

half-open-idle-timeout

Description Enables the configuration of half-open TCP sessions. A half-open refers to the TCP session in which the client receives a SYN-ACK, but does not reply with an ACK.

This mode is supported only for client side data streams.

Syntax

```
[no] half-open-idle-timeout num
```

Parameter	Description
num	Number of seconds (1-60).

Default Not set.

Mode SLB TCP template

Example Set the timeout to 60 seconds.

```
ACOS(config)# slb template tcp tcp-tmp1
ACOS(config-l4 tcp)# half-open-idle-timeout 60
```

idle-timeout

Description Specifies the number of minutes that a connection can be idle before the ACOS device terminates the connection.

Syntax

```
[no] idle-timeout num
```

Parameter	Description
num	Number of seconds (1-2097151, about 24 days). • For values less than 31, ACOS uses the entered value. • For values between 31 and 60, ACOS rounds up to 60 seconds. • For values greater than 60, ACOS rounds down to the closest multiple of 60 seconds.

Default 120 seconds

Mode SLB TCP template

Example Set the idle timeout to 60 seconds.

```
ACOS(config)# slb template tcp tcp-tmp1
ACOS(config-l4 tcp)# idle-timeout 60
```

initial-window-size

Description Sets the initial TCP window size in SYN ACK packets to clients. The TCP window size in a SYN ACK or ACK packet specifies the amount of data that a client can send before it needs to receive an ACK.

The initial TCP window size applies only to the SYN ACKs sent to the client. After the SYN ACK, the ACOS device does not modify the TCP window size for any other packets in the session.

By default, the ACOS device uses the TCP window size set by the client or server:

Syntax

```
[no] initial-window-size num
```

Parameter	Description
num	Window size in bytes (1-65535).

Mode SLB TCP template

Example Set the initial TCP window size to 256.

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# initial-window-size 256
```

insert-client-ip

Description Inserts the client IP address into an options field in the TCP header.

This option is useful for applications that require knowledge of the client IP address, but that do not use HTTP or another protocol such as Financial Information eXchange (FIX) that can include this information.

For example, insertion of the client IP address into the TCP header can be useful for financial applications that do not use FIX.

When this feature is enabled, ACOS places the client IP address into a TCP option field of type 0x1c, with a length of 7 bytes. For example, the value placed by ACOS into the TCP header for client 40.40.40.26 is 0x1c07012828281a.

Syntax `[no] insert-client-ip`

Default Not enabled

Mode SLB TCP template

Example Enable this feature.

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# insert-client-ip
```

lan-fast-ack

Description Increases performance of bidirectional peer sessions by acknowledging receipt of data on behalf of clients and servers.

Syntax `[no] lan-fast-ack`

Default Not enabled

Mode SLB TCP template

Example Enable this feature.

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# lan-fast-ack
```

proxy-header

Description Configures proxy protocol header insertion only. For more information on proxy protocol, refer HAProxy.

NOTE:

This feature is not supported for fast Path and UDP. Additionally, this feature cannot be configured with the following functionality:

- aflex with TCP payload replace
- Fast-fix with client ip insert
- FTP virtual port

Syntax

```
[no] proxy-header insert {v1 | v2}]
```

Parameter	Description
v1	Specifies the header in human-readable (ASCII string) format.
v2	Specifies the header in binary format.

Default Not configured.

Mode SLB TCP template mode

Usage The following process explains how the proxy protocol interacts with the ADC:

1. Enable proxy protocol in the ADC instance and connect it to the service.
2. The appliance determines the proxy protocol version on the sending side based on CLI configuration.
3. ADC inserts a proxy header containing client connection information and passes it to the backend server.

Example This command configures TCP template with version 1, then bind it to vport.

NOTE: The proxy-header option will take effect only when the TCP template is bound under TCP virtual port.

```
ACOS(config)# slb template tcp TP
ACOS(config-tcp proxy)# proxy-header insert v1
ACOS(config-tcp proxy)# exit
ACOS(config)# slb virtual-server VIP-10 10.1.1.1
ACOS(config-slb vserver)# port 80 tcp
```

```
ACOS(config-slb vserver-vport)# template tcp TP
```

Related Commands:

- Under SLB TCP Proxy Template: proxy-header

qos

Description Marks DSCP (Layer 3) and 802.1p priority (Layer 2) values in client-server SLB traffic.

Syntax

```
[no] qos num
```

Parameter	Description
num	Values range between 1 to 63. Based on the value you specify, ACOS marks the traffic as follows: • Layer 3 marking – ACOS sets Diffserv Control Point (DSCP) value in IP header to specified value. • Layer 2 marking – ACOS sets 802.1p value in MAC header to the value you specify, divided by 9.

Mode SLB TCP template

Example Set the QOS value to 63:

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# qos 63
```

reset-follow-fin

Description enables closing a client or server connection with a reset (RST) on the first FIN received from the client or server.

Syntax

```
[no] reset-follow-fin
```

Default Not enabled.

Mode SLB TCP template

Usage This option alleviates the situation where a backend server receives the client FIN, ACKs the FIN, enters CLOSE_WAIT but does not close the

connection (no-FIN behavior), which can result in a build-up of CLOSE-WAIT sessions and the subsequent resource exhaustion on the server.

Example Enable this feature:

```
ACOS(config)# slb template TCP TCP-TEMP
ACOS(config-l4 tcp)# reset-follow-fin
ACOS(config-l4 tcp)#
```

reset-fwd

Description Sends a TCP RST to the real server after a session times out.

Syntax

```
[no] reset-fwd
```

Default Not enabled.

Mode SLB TCP template

Example Enable this feature:

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# reset-fwd
```

reset-rev

Description Sends a TCP RST to the client after a session times out.

This command does not send an RST if a server selection failure occurs. To do this, use the **reset-on-server-selection-fail** option at the configuration level for the service group or virtual port.

Syntax

```
[no] reset-rev [STATE]
```

Parameter	Description
STATE	• **disable** - Send the TCP RST only when the server is Disabled. • **down** - Send the TCP RST only when a server is Down. When no option is specified, TCP RST is sent for any error

Default Not enabled.

Mode SLB TCP template and SLB TCP Proxy template

Usage If the server is Down, the reset-rev option immediately sends the RST to the client and does not wait for the session to time out.

When using reset-rev disable with the disable-with-hm command under SLB server configuration, the server is not treated as “disabled” since persist sessions continue to use the “disabled” server.

When using reset-rev disable with the slb graceful-shutdown Global configuration command, state of enabled is also not treated as disabled but as UP since existing sessions need to be drained and not reset.

Example Enable this feature in SLB TCP Template:

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# reset-rev
```

Example Enable this feature in SLB TCP Proxy Template:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# reset-rev
```

slb template tcp-proxy

Description Configure TCP/IP stack parameters.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all virtual ports that use the template.

Syntax `[no] slb template tcp-proxy {default | template-name}`

Parameter	Description
default	Edit the default TCP proxy template. This template can be modified in the same way as any custom *template-name* you specify.
template-name	Template name (1-127 characters)

This command enters the SLB TCP Proxy Template Configuration Mode Commands for the specified TCP-Proxy template.

Mode Configuration mode

Usage The normal form of this command creates a TCP-proxy configuration template. The **no** form of this command removes the template.

You can bind only one TCP-proxy template to a virtual port. However, you can bind the same TCP-proxy template to multiple ports.

Example The following commands create a TCP-proxy template named “rst” and sets the idle timeout to 3000 seconds: When the idle timeout occurs, the ACOS device will send an RST to the client. In cases where the server goes down, the ACOS device will reset the connection.

```
ACOS(config)# slb template tcp-proxy rst
ACOS(config-tcp proxy)# idle-timeout 3000
ACOS(config-tcp proxy)# reset-rev
ACOS(config-tcp proxy)# server-down-action RST
```

proxy-header

Description Configures proxy protocol header insertion only. For more information, see HAProxy.

NOTE: This command should be configured in the named TCP proxy template and not recommended to configure in the **default** TCP proxy template.

Syntax

```
[no] proxy-header insert {v1 | v2}
```

Parameter	Description
v1	Specifies the header in human-readable (ASCII string) format.
v2	Specifies the header in binary format.

Default Not configured.

Mode SLB TCP Proxy template mode

Example This command is configured in a TCP proxy template named TP with version 1, then bound to the virtual port.

```
ACOS(config)# slb template tcp-proxy TP
ACOS(config-tcp proxy)# proxy-header insert v1
ACOS(config-tcp proxy)# exit
ACOS(config)# slb virtual-server VIP-10 10.1.1.1
ACOS(config-slb vserver)# port 80 tcp-proxy
ACOS(config-slb vserver-vport)# template tcp-proxy TP
```

Related Commands:

- SLB SIP template: insert-client-ip
- SLB TCP template: insert-client-ip
- SLB TCP proxy template: insert-client-ip

ack-aggressiveness

Description Specifies the cases in which the ACOS device sends an ACK to the client.

A high ACK aggressiveness helps reduce the delay of interactive client-server applications, but at a cost of more ACKs.

Syntax

```
[no] ack-aggressiveness {high | medium | low}
```

Parameter	Description
high	Send ACK for each packet.
medium	Delayed ACK, with ACK on each packet with PUSH flag.
low	Delayed ACK.

Default low

Mode SLB TCP proxy template

Example Set the ACK aggressiveness level to medium:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# ack-aggressiveness medium
```

backend-wscale

Description Specifies the TCP window scaling factor for backend connections to servers.

The TCP window scaling factor is applicable to virtual ports for which the ACOS device acts as a TCP proxy.

The TCP window scaling factor is used to calculate the TCP receive window, which is the maximum amount of data (in bytes) the receiver on a TCP connection will buffer. The sender is not allowed to send more than this amount of data before receiving an acknowledgement that the data has arrived.

Syntax

```
[no] backend-wscale num
```

Parameter	Description
num	Scaling factor (1-14).

Default Disabled

Mode SLB TCP proxy template

Example Set the scaling factor to 3.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# backend-wscale 3
```

del-session-on-server-down

Description This command clears a port protocol session within 2 to 3 seconds if a session server is disabled by ACOS command or the server fails an ACOS health check at the service group level.

If a one or more real servers in a service group fails the health check and this command is enabled for the session, ACOS clears the session.

Active sessions, (receiving client-side packets) clear within 2 to 3 seconds. Idle sessions may continue to exist for over a minute after the command is issued.

Syntax

```
[no] del-session-on-server-down
```

Default This feature is disabled by default.

Mode SLB TCP proxy template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# del-session-on-server-down
```

disable-abc

Description Calculates the Congestion Window based on appropriate counting of the bytes (ABC). It is recommended that ABC is enabled.

Syntax

```
[no] disable-abc
```

Default This feature is enabled by default.

Mode SLB TCP proxy template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# disable-abc
```

disable-sack

Description Disables flows to use Selective Ack options, which are sent by the receiver to inform the sender of missing data segments to enhance TCP fast recovery.

Syntax

```
[no] disable-sack
```

Default This feature is enabled by default.

Mode SLB TCP proxy template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# disable-sack
```

disable-tcp-timestamps

Description Disables the TCP Timestamps option. Disabling this option stops the TCP Protection Against Wrapping Sequence (PAWS) and causes retransmission timeout (RTO) calculations to use relative receive time for round-trip time (RTT) calculations.

Syntax

```
[no] disable-tcp-timestamps
```

Default This feature is enabled by default.

Mode SLB TCP proxy template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# disable-tcp-timestamps
```

disable-window-scale

Description Disables the TCP Window-Scale option. Disabling the Window-Scale option prevents an increase in the amount of data that the receiver can accept before sending an acknowledgement to the sender.

Syntax

```
[no] disable-window-scale
```

Default This feature is enabled by default.

Mode SLB TCP proxy template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# disable-window-scale
```

do-newsack

Description Configures the selective ACK options for fast loss recovery in TCP connections.

Syntax

```
[no] do-newsack {enable | disable | auto-select}
```

Parameter	Description
enable	Enable fast selective ACK loss recovery.
disable	Disable fast selective ACK loss recovery.
auto-select	Auto select fast selective ACK loss recovery (disable).

Default Auto-select

Mode SLB TCP proxy template

Usage Adjusts slowstart threshold more efficiently enabling faster recovery from packet loss.

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy tcp2
ACOS(config-tcp proxy)# do-newsack enable
```

dynamic-buffer-allocation

Description Optimally adjusts the transmit and receive buffer sizes of TCP-proxy while maintaining a constant sum of combined values.

Syntax

```
[no] dynamic-buffer-allocation
```

Default Not enabled

Mode SLB TCP proxy template

Example Enable the feature.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# dynamic-buffer-allocation
```

early-retransmit

Description Specifies the number of packets that an ACOS device sends when it retransmits lost data.The recommended setting is 3. This allows problematic networks time to recover from data loss before attempting another transmission.

Syntax

```
[no] early-retransmit num
```

Parameter	Description
num	Number of data packets (1-3).

Default 3

Mode SLB TCP proxy template

Example Set the size of retransmitted packets to 3:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# early-retransmit 3
```

fin-timeout

Description Specifies the number of seconds that a connection can be in the FIN-WAIT2 or LAST-ACK state before the ACOS device terminates the connection.

Syntax

```
[no] fin-timeout num
```

Parameter	Description
num	Timeout in seconds (1-60).

Default Disabled

Usage This command can be used as countdown to clients in the FIN-WAIT2 or LAST-ACK state. However, for the last FIN-ACK state, the command must be set to a value between 1-30 seconds only.

Mode SLB TCP proxy template

Example The following commands create a TCP-proxy template named “rst” and sets the `fin-timeout` to 30 seconds. When the last FIN-ACK occurs, the ACOS device will wait for 30 seconds before removing the client connection.

```
ACOS(config)# slb template tcp-proxy rst
ACOS(config-tcp proxy)# fin-timeout 30
```

force-delete-timeout

Description Specifies maximum number of seconds a session can remain active, and forces deletion of any session that is still active after the specified number of seconds.

This option is useful for small, fast transactions for which the completion time of sessions is guaranteed. When used in combination with the reset-fwd and reset-rev commands, this option can help clean up user connections with RSTs instead of allowing the connections to hang.

Syntax

```
[no] force-delete-timeout num [alive-if-active]
```

Parameter	Description
num	Number of seconds (1-31).
alive-if-active	Terminates half-open TCP sessions on the virtual port while allowing active sessions to continue without being terminated.

Mode SLB TCP proxy template

Example Set the timeout to 10 seconds.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# force-delete-timeout 10
```

force-delete-timeout-100ms

Description Specifies the maximum number of milliseconds a session can remain active, and forces deletion of any session that is still active after the specified number of milliseconds.

Syntax

```
[no] force-delete-timeout-100ms num [alive-if-active]
```

Parameter	Description
num	Number of 100ms units (1-31).
alive-if-active	Terminates half-open TCP sessions on the virtual port while allowing active sessions to continue without being terminated.

Mode SLB TCP proxy template

Example Set the timeout to 10 100-milliseconds (1 second).

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# force-delete-timeout-100ms 10
```

half-close-idle-timeout

Description Enables aging of half-closed TCP sessions. A half-closed refers to the TCP session in which the server sends a FIN but the client does not reply with an ACK.

The ACOS device keeps half-closed sessions open indefinitely.

Syntax

```
[no] half-close-idle-timeout num
```

Parameter	Description
num	Number of seconds (60-120).

Default Not set.

Mode SLB TCP template

Example Set the timeout to 60 seconds.

```
ACOS(config)# slb template tcp default
ACOS(config-tcp proxy)# half-close-idle-timeout 60
```

half-open-idle-timeout

Description Enables aging of half-open TCP sessions. A half-open TCP session is one in which the client receives a SYN-ACK, but does not reply with an ACK.

This command is supported only on the client side.

NOTE: The **half-close-idle-timeout** command is deprecated. Hence, instead of this command you can use **fin-timeout** command.

Syntax

```
[no] half-open-idle-timeout num
```

Parameter	Description
num	Number of seconds (1-60).

Mode SLB TCP proxy template

Example Set the timeout to 60 seconds.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# half-open-idle-timeout 60
```

idle-timeout

Description Specifies the number of minutes that a connection can be idle before the ACOS device terminates the connection.

Syntax

```
[no] idle-timeout num
```

Parameter	Description
num	Number of seconds (1-2097151, about 24 days). • For values less than 31, ACOS uses the entered value. • For values between 31 and 60, ACOS rounds up to 60 seconds. • For values greater than 60, ACOS rounds down to the closest multiple of 60 seconds.

Default 600 seconds

Mode SLB TCP proxy template

Usage See keepalive-interval for more information about how the idle timeout and keepalive values are related.

Example Set the idle timeout to 60 seconds.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# idle-timeout 60
```

init-cwnd

Description Specifies the maximum number of unacknowledged packets that can be sent on a TCP connection. A large initial congestion-control window size helps reduce HTTP response latency, especially for short web pages.

Syntax

```
[no] init-cwnd num
```

Parameter	Description
num	Number of unacknowledged packets (1-15)..

Default 10

Mode SLB TCP proxy template

Example Set the initial congestion-window size to 12.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# init-cwnd 12
```

initial-window-size

Description Sets the initial TCP window size in SYN ACK packets to clients. The TCP window size in a SYN ACK or ACK packet specifies the amount of data that a client can send before it needs to receive an ACK.

The initial TCP window size applies only to the SYN ACKs sent to the client. After the SYN ACK, the ACOS device does not modify the TCP window size for any other packets in the session.

By default, the ACOS device uses the TCP window size set by the client or server:

- If the virtual port is one of the service types that is proxied by the ACOS device, initial TCP window size applies to SYN ACKs generated by the ACOS device and sent to clients. By default, the ACOS device uses the TCP window size in the client's SYN. The following service types are proxied by the ACOS device: HTTP, HTTPS, Fast-HTTP, SSL-proxy, and SMTP.
- If the virtual port is not one of the service types that is proxied by the ACOS device (for example, the tcp service type), initial TCP window size applies to SYN ACKs generated by servers and

forwarded by the ACOS device to clients. By default, the ACOS device uses the TCP window size in the server's SYN ACK.

If SYN cookies are enabled, either globally or on the virtual service port, the ACOS device acts as a TCP proxy even though the service type is not normally proxied. In this case, the behavior is the same as for any of the other service types TCP proxied by the ACOS device

Syntax

```
[no] initial-window-size num
```

Parameter	Description
num	Window size in bytes (1-65535).

Mode SLB TCP proxy template

Example Set the initial TCP window size to 256.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# initial-window-size 256
```

insert-client-ip

Description Inserts the client IP address into an options field in the TCP header.

This option is useful for applications that require knowledge of the client IP address, but that do not use HTTP or another protocol such as Financial Information eXchange (FIX) that can include this information.

For example, insertion of the client IP address into the TCP header can be useful for financial applications that do not use FIX.

When this feature is enabled, ACOS places the client IP address into a TCP option field of type 0x1c, with a length of 7 bytes. For example, the value placed by ACOS into the TCP header for client 40.40.40.26 is 0x1c07012828281a.

Syntax

```
[no] insert-client-ip
```

Default Not enabled

Mode SLB TCP proxy template

Example Enable this feature.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# insert-client-ip
```

invalid-rate-limit

Description Limits the rate at which responses are sent (in milliseconds) for suspicious or invalid packets.

Syntax

```
[no] invalid-rate-limit num
```

Parameter	Description
num	Limit invalid packet responses in milliseconds (0-60000000).

Default 500 ms

Mode SLB TCP proxy template

Example This example shows how the command is applied:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# invalid-rate-limit 700
```

keepalive-interval

Description Number of seconds a TCP-proxy session can remain idle before the ACOS device sends a TCP ACK to the devices on both ends of the session.

Syntax

```
[no] keepalive-interval num
```

Parameter	Description
num	Keepalive interval in seconds (60-12000).

Default Not set

Mode SLB TCP proxy template

Usage The keepalive feature, which for TCP-proxy templates, periodically verifies that a TCP-proxy session is still up on both ends of the session. The keepalive feature uses keepalive interval to establish the number of

seconds a TCP-proxy session can remain idle before the ACOS device sends a TCP ACK to the devices on both ends of the session, and the keepalive probe count allows you to set the maximum number of times the ACOS device sends a keepalive ACK, before deleting the session.

The ACOS device sends the first keepalive ACK if a session remains idle for the duration of the keepalive interval:

- If both devices respond with an ACK before the next keepalive interval expires, the ACOS device resets the keepalive time to 0. This starts a new keepalive interval.
- If either device does not respond with an ACK before the next keepalive interval expires, the action taken by the ACOS device depends on the setting of the keepalive probe count.
  - Keepalive probe count set to value greater than 1 – The ACOS device sends another ACK to each device.

    - If both devices respond, the ACOS device resets the keepalive time to 0, to begin a new keepalive interval.

    - If either device does not respond, the ACOS device sends another ACK to each device. This action can be repeated up to the configured maximum number of probes (the probe count).
  - Keepalive probe count set to 1 – The ACOS device does not send new probe ACKs. Instead, the ACOS device deletes the session.

Relation of Keepalive to Idle-timeout

The keepalive and idle-timeout options work independently of one another.

By default, the keepalive interval is shorter than the idle timeout. In this case, keepalive probes are triggered before the idle timeout expires.

- If both devices respond with an ACK *before* either of the following occurs, the keepalive interval time and the idle time are both reset to 0.
  - Idle timeout expires – If this occurs, the session is deleted, even if the maximum number of keepalive probes have not been sent.

- Maximum number of keepalive probes are sent, but at least one of the devices still does not respond – In this case, the session is deleted even if the idle timeout has not expired.

- If you change the keepalive or idle-timeout settings so that the idle timeout is shorter than the keepalive interval, the keepalive mechanism is never triggered. The idle timeout always expires first, causing the session to be deleted. No keepalive probes are ever sent.

Example Set the keepalive interval to 120 seconds.

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# keepalive-interval 120
```

keepalive-probes

Description Maximum number of times the ACOS device sends a keepalive ACK, before deleting the session.

Syntax

```
[no] keepalive-probes num
```

Parameter	Description
num	Number of keepalive probes (2-10).

Default Not set

Mode SLB TCP proxy template

Example Send 5 keepalive ACKs before deleting the session:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# keepalive-probes 5
```

limited_slowstart

Description Specifies the maximum amount of data the ACOS device initially transmits in an effort to promote a healthy network connection and avoid congestion.

Syntax

```
[no] limit-slowstart num
```

Parameter	Description
num	Amount of data transmitted during a TCP slow start (0-2147483647 bytes).

Default 0

Mode SLB TCP proxy template

Example Set the size of the TCP slow start to 500 bytes:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# limit-slowstart 500
```

maxburst

Description Limits that number of data segments that can be transmitted for each TCP window the ACOS device sends.

Syntax

```
[no] maxburst num
```

Parameter	Description
num	Number of segments transmitted (1-100).

Default 25

Mode SLB TCP proxy template

Example Set the number of segments transmitted 100:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# maxburst 100
```

min-rto

Description Specifies the minimum length of time for an ACOS device to transmit data and receive acknowledgement that the data was received. This configuration is particularly helpful in networks with low bandwidth. Increase the length of time for low bandwidth.

Syntax

```
[no] min-rto num
```

Parameter	Description
num	Length of time (in milliseconds) to complete data transmission and ACK (100-1000 milliseconds).

Default 200 milliseconds

Mode SLB TCP proxy template

Example Set the length of time (in milliseconds) for round-trip data transmission to 500:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# min-rto 500
```

mss

Description Change the minimum supported TCP Maximum Segment Size (MSS).

Syntax

```
[no] mss num
```

Parameter	Description
num	TCP maximum segment size in octets (128-1460).

Default 1460

Mode SLB TCP proxy template

Example Set the MSS to 1460:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# mss 1460
```

nagle

Description Enables Nagle congestion compression (described in RFC 896).

Syntax

```
[no] nagle
```

Default Not enabled

Mode SLB TCP proxy template

Example Enable the feature:

```
ACOS(config)# slb template tcp-proxy PROXY1
ACOS(config-tcp proxy)# nagle
ACOS(config-tcp proxy)#
```

naked-ack-on-handshake

Description Enable naked ACK flag on the TCP-Proxy template.

Syntax

```
[no] naked-ack-on-handshake
```

Default Not enabled

Mode SLB TCP proxy template

Usage With this feature, the TCP handshake will complete only with a naked ACK (or 'pure' ACK) packet before any data gets sent.

This is useful when you need an option to disable piggybacking on the last ACK especially in the case of SSLi or Explicit proxy environments. However, most modern server implementations do not require naked ACK as it increases the traffic overhead for transmitting extra packets.

Example The following command enables the feature:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# naked-ack-on-handshake
```

psh-flag-optimization

Description Enables PSH flag optimization on the configuration mode TCP-Proxy template.

The PSH (PUSH) flag is a TCP option that allows an application to start sending the data even if the buffer is not full. By default, the PSH flag uses the PSH setting on every data segment. To limit its use for SSL flows, the ssl flush routine is modified to mark the last buffer within the queue with a psh marker. When PSH Flag Optimization is enabled, TCP reads the PSH marker and sets the PSH flag on packets based on that marker..

Syntax

```
[no] psh-flag-optimization
```

Default Not enabled

Mode SLB TCP proxy template

Example This example enables the feature:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# psh-flag-optimization
ACOS(config-tcp proxy)#
```

qos

Description Marks the DSCP (Layer 3) and 802.1p priority (Layer 2) values in client-server SLB traffic.

Syntax

```
[no] qos num
```

Parameter	Description
num	You can set a value between 1 to 63. Based on the value you specify, ACOS marks the traffic as follows: • Layer 3 marking – ACOS sets the Diffserv Control Point (DSCP) value in the IP header to value you specify. • Layer 2 marking – ACOS sets the 802.1p value in the MAC header to the value you specify, divided by 9.

Mode SLB TCP proxy template

Example Set the QOS value to 63:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# qos 63
```

reassembly-limit

Description Specifies the maximum number of TCP segments allowed in the assembly queue for each flow.

Syntax

```
[no] reassembly-limit num
```

Parameter	Description
num	Number of segments allowed (1-500).

Default 25

Mode SLB TCP proxy template

Example Limit number of reassembly segments to 100:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# reassembly-limit 100
```

reassembly-timeout

Description Specifies the length of time (in seconds) that the ACOS device waits for progress to be made in the reassembly of TCP segments before it removes segments from the assembly queue.

Syntax

```
[no] reassembly-timeout num
```

Parameter	Description
num	Number of seconds before TCP segments are removed if reassembly does not occur successfully (1-300 seconds).

Default 30 seconds

Mode SLB TCP proxy template

Example Set reassembly limit to 120:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# reassembly-timeout 120
```

receive-buffer

Description Specifies the maximum number of bytes addressed to the port that the ACOS device will buffer.

Syntax

```
[no] receive-buffer num
```

Parameter	Description
num	Number of bytes to buffer (1-2147483647).

Default 200000 (200KB)

Mode SLB TCP proxy template

Example Set the buffer size to 51200:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# receive-buffer 51200
```

reno

Description Enables the TCP Reno congestion control algorithm, and disables Cubic.

Syntax

```
[no] reno
```

Default Not enabled; Cubic is used by default

Mode SLB TCP proxy template

Example Enable TCP Reno congestion control algorithm:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# reno
```

reset-fwd

Description Sends a TCP RST to the real server after a session times out.

Syntax

```
[no] reset-fwd
```

Mode SLB TCP proxy template

Example Enable this feature:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# reset-fwd
```

reset-rev

Description Sends a TCP RST to the client after a session times out.

Syntax `[no] reset-rev [STATE]`

Parameter	Description
STATE	• **disable** - Send TCP RST only when the server is Disabled. • **down** - Send the TCP RST only when a server is Down. When no option is specified, TCP RST is sent for any error.

Mode SLB TCP proxy template

Usage If the server is Down, the reset-rev option immediately sends the RST to the client and does not wait for the session to time out.

When using reset-rev disable with the disable-with-hm command under SLB server configuration, the server is not treated as “disabled” since persist sessions continue to use the “disabled” server.

When using reset-rev disable with the slb graceful-shutdown Global configuration command, state of enabled is also not treated as disabled but as UP since existing sessions need to be drained and not reset.

Default Not enabled.

retransmit-retries

Description Specifies the maximum number of times the ACOS device can retransmit a data segment for which the ACOS device does not receive an ACK.

Syntax `[no] retransmit-retries num`

Parameter	Description
num	Number of retries (1-20).

Default 5

Mode SLB TCP proxy template

Example Configure 3 retry attempts:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# retransmit-retries 3
```

syn-retries

Description Specifies the maximum number of times the ACOS device can retransmit a SYN for which the ACOS device does not receive an SYN-ACK.

Syntax

```
[no] syn-retries num
```

Parameter	Description
num	Number retries (1-20).

Default 5

Mode SLB TCP proxy template

Usage When an SYN packet is sent, the TCP syn-retries value is initiated. If no response packet is received after the specified time, the TCP connection is closed. By default, the server auto-reselection is enabled. In this case, the number of syn-retry attempts uses the following formula:

Syn-retries divided by the number of service-group members is equal to the number of syn-retry attempts. For example, 10 (syn-retries) / 2 (service-group members) = 5 attempts.

Example Configure 7 retry attempts:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# syn-retries 7
```

timewait

Description Specifies the number of seconds that a connection can be in the TIME-WAIT state before the ACOS device transitions it to the CLOSED state.

Syntax

```
[no] timewait num
```

Parameter	Description
num	Number of seconds (1-60).

Default 5 seconds

Mode SLB TCP proxy template

Example Set the timewait interval to 7 seconds:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# timewait 7
```

transmit-buffer

Description Specifies the maximum number of bytes sent by the port that the ACOS device will buffer.

Syntax

```
[no] transmit-buffer num
```

Parameter	Description
num	Number of bytes to buffer (1-2147483647).

Default 200000 (200KB)

Mode SLB TCP proxy template

Example Set the buffer size to 51200 bytes:

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# transmit-buffer 51200
```

slb template udp

Description Configure UDP connection settings.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all virtual ports that use the template.

Syntax

```
[no] slb template udp {default | template-name}
```

Parameter	Description
default	Edit the default SLB UDP template. This template can

Parameter	Description
	be modified in the same way as any custom *template-name* you specify.
template-name	Template name (1-127 characters)

This command enters the SLB UDP Template Configuration Mode Commands for the specified UDP template.

Mode Configuration mode

Usage The normal form of this command creates a UDP configuration template. The **no** form of this command removes the template.

You can bind only one UDP template to a virtual port. However, you can bind the same UDP template to multiple ports.

Example The following commands create a UDP template named "udp-quickterm" and set session termination to occur immediately after a response is received:

```
ACOS(config)# slb template udp udp-quickterm
ACOS(config-l4 udp)#aging immediat
```

Related Commands

- lb-method-hash

aging

Description Specifies how quickly sessions are terminated when the request is received.

Syntax

```
[no] aging {immediate | short [seconds]}
```

Parameter	Description
immediate	• Response Received—Session is terminated within 1 second. • No Response—Idle timeout value in UDP template is used.

Parameter	Description
short	• Response Received—Session is terminated within 1 second. • No Response—Session is terminated after configured short aging period (1-30 seconds).

NOTE: Best Practice is to explicitly set aging in UDP templates used by DNS virtual ports.

Default Not set by default; the default behavior is:

- Response Received—Behavior depends on the port number:
  - Port 53 (default DNS port)—Session terminates within 1 second.
  - Any other port number—Session terminates after idle timeout expires.
- No Response— Idle timeout value in UDP template is used.

Mode SLB UDP template

Example Configure immediate aging:

```
ACOS(config)# slb template udp udp-tmp1
ACOS(config-l4 udp)# aging immediate
```

idle-timeout

Description Specifies the number of seconds a connection can remain idle before the ACOS device terminates the connection.

Syntax

```
[no] idle-timeout num
```

Parameter	Description
num	Number of seconds (1-2097151, about 24 days). • For values less than 31, ACOS uses the entered value. • For values between 31 and 60, ACOS rounds up to 60 seconds.

Parameter	Description
	• For values greater than 60, ACOS rounds down to the closest multiple of 60 seconds.

The maximum idle timeout supported for TFTP virtual ports is 15300 seconds (255 minutes).

Default 120 seconds

Mode SLB UDP template

Example Set the idle timeout to 300 seconds (5 minutes):

```
ACOS(config)# slb template udp udp-tmp1
ACOS(config-l4 udp)# idle-timeout 300
```

qos

Description Marks the DSCP (Layer 3) and 802.1p priority (Layer 2) values in client-server SLB traffic.

Syntax

```
[no] qos num
```

Parameter	Description
num	Sets a value between 1 to 63. Based on the value you specify, ACOS marks the traffic as follows: • Layer 3 marking – ACOS sets Diffserv Control Point (DSCP) value in IP header to specified value. • Layer 2 marking – ACOS sets 802.1p value in MAC header to the specified value divided by 9.

Mode SLB UDP template

Example Set the QOS value to 54:

```
ACOS(config)# slb template udp udp-tmp1
ACOS(config-l4 udp)# qos 54
```

radius-lb-method

Description Configure the RADIUS load balancing method.

Syntax

```
[no] radius-lb-method hash {ip [avp 4 | 8]| ipv6 [avp 97 | 168] }
```

Parameter	Description
hash {ip |ipv6}	Specify the hashing type. Currently, only the IP hashing methodology is supported.
avp [{*4* | *8*} | {*97* | *168*}]	Specifies the RADIUS Attribute Value Pairs (AVP) number. The following AVP types are available for hash ip: • 4 - Specifies NAS-IP-Address. • 8 - Specifies Framed-IP-Address. The following AVP types are available for hash ipv6: • 97 - Specifies Framed-IPv6-Prefix. • 168 - Specifies Framed-IPv6-Address.

Mode SLB UDP template

Usage Configures the RADIUS load-balancing method. ACOS receives various RADIUS requests for multiple clients with the same source and destination addresses. If a RADIUS virtual port is used, the ACOS device uses the configured load balancing method to select a server for the first request, then uses the same server (and data CPU) for all subsequent requests.

Example The following commands create a UDP template named "udp-radius" and defines the load balancing method to be used. Only ip-based hash method is supported. For IPv4, the AVP number is a Radius attribute (8=Framed IP and 4= NAS-IP) of the source IP. The syntax of this command is as follows:

```
[no] radius-lb-method | hash |ip | avp | {4 , 8}
```

The example is as follows:

```
ACOS(config)# slb template udp udp-radius
ACOS(config-l4 udp)# radius-lb-method hash ip avp 8
```

Example The following commands create a UDP template named "udp-radius1" and defines the load balancing method to be used. Only ip-based hash method is supported. For IPv6, the AVP number is a Radius attribute (97=Framed-IPv6-Prefix and 168= Framed-IPv6-Address) of the source IP. The syntax of this command is as follows:

```
[no] radius-lb-method | hash |ip | avp | {97 , 168}
```

The example is as follows:

```
ACOS(config)# slb template udp udp-radius1
ACOS(config-l4 udp)# radius-lb-method hash ipv6 avp 168
```

re-select-if-server-down

Description Configures the ACOS device to select another real server if the server that is bound to an active connection goes down. Without this option, another server is not selected.

By default, the device clears all UDP sessions from the server that goes down.

Syntax

```
[no] re-select-if-server-down [disable-clear-session]
```

Parameter	Description
disable-clear-session	When this option is enabled, the device does not immediately clear sessions from a server that goes down.

Default Not enabled.

Mode SLB UDP template

Example These commands configures the device to select another real server when a server bound to an active connection goes down and clears all UDP sessions for the disabled server.

```
ACOS(config)# slb template udp udp-tmp1
ACOS(config-l4 udp)# re-select-if-server-down
```

stateless-conn-timeout

Description Set the stateless current connection timeout value in seconds.

Syntax

```
[no] stateless-conn-timeout num
```

Parameter	Description
num	Stateless connection timeout value in seconds (5-120).

Default 120 seconds

Mode SLB UDP template

Example Set the stateless connection timeout to 60 seconds.

```
ACOS(config)# slb template udp udp-tmp1
ACOS(config-l4 udp)# stateless-conn-timeout 60
```

slb template virtual-port

Description Configure a template of SLB settings for virtual service ports.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all virtual ports that use the template.

Syntax

```
[no] slb template virtual-port {default | template-name}
```

Parameter	Description
default	Edit the default virtual port template. This template can be modified similar to any custom *template-name* you specify.
template-name	Template name (1-127 characters)

This command enters the SLB Virtual Port Template Configuration Mode Commands for the specified Virtual-Port template.

Mode Configuration mode

Usage The normal form of this command creates a virtual service port template. The **no** form of this command removes the template.

You can bind only one virtual service port template to a virtual service port. However, you can bind the virtual service port template to multiple virtual service ports.

Some of the parameters that can be set using a template can also be set or changed on the individual virtual port.

- If a parameter is set (or changed from its default) in both a template and on the individual virtual port, the setting on the individual virtual port takes precedence.
- If a parameter is set (or changed from its default) in a template but not set or changed from its default on the individual virtual port, the template setting takes precedence.

Example These commands configure a virtual service port template named “common-vpsettings”, set the connection limit, and bind the template to a virtual port:

```
ACOS(config)# slb template virtual-port common-vpsettings
ACOS(config-vport)# conn-limit 500000
ACOS(config-vport)# exit
ACOS(config)# slb virtual-server vip1 10.10.10.99
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template virtual-port common-vpsettings
```

Example The following commands create real servers “s1” at 5.5.5.1 (with a real port range of 10), real server “s2” at 5.5.5.2 (with a range of 25), and real server “s3” at 5.5.5.3 (which does not have a range configured and will not be used for this feature). These real servers are then bound to a service group “sg1”, which is in turn, bound to a VIP (“vip3”) at 10.10.10.0 /24. A virtual port template “vport1” is created, and the

allow-vip-to-rport-mapping option is used, and the template is bound to the “vip3”.

```
ACOS(config)# slb server s1 5.5.5.1
ACOS(config-real server)# port 80 tcp range 10
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server s2 5.5.5.2
ACOS(config-real server)# port 80 tcp range 25
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server s3 5.5.5.3
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg1 tcp
ACOS(config-slb svc group)# member s1 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s2 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s3 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# allow-vip-to-rport-mapping
ACOS(config-vport)# exit
ACOS(config)# slb virtual-server vip3 10.10.10.0 /24
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# service-group sg1
ACOS(config-slb vserver-vport)# template virtual-port vport1
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# port 90 http
ACOS(config-slb vserver-vport)# service-group sg1
ACOS(config-slb vserver-vport)# template virtual-port vport1
ACOS(config-slb vserver-vport)# exit
```

aflow

Description Enables aFlow control. aFlow helps avoid packet drops and retransmissions when a real server port reaches its configured

connection limit. aFlow control is triggered when the following occurs:

- If connection limit is configured on the real server or real port – The backend real server or real port reaches its configured connection limit.

When aFlow is enabled, the ACOS device queues HTTP/HTTPS packets from clients when a server port reaches a configured connection limit, instead of dropping them. The ACOS device then monitors the port, and begins forwarding the queued packets when connections become available again. To prevent flooding of the port, the ACOS device forwards the queued packets at a steady rate.

aFlow applies only to HTTP and HTTPS virtual ports.

Syntax `[no] aflow`

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport-tmplt1
ACOS(config-vport)# aflow
```

allow-syn-otherflags

Description Allows initial SYN packet with other flags.

Syntax `[no] allow-syn-otherflags`

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport-tmplt1
ACOS(config-vport)# allow-syn-otherflags
```

allow-vip-to-rport-mapping

Description Enables the VIP to Real Port Mapping feature for a subnet VIP.

The virtual port template containing this option must be bound to the VIP, and the VIP itself must use a subnet for the last octet (for example,10.10.10.0 /24), or the feature will not work.

Syntax `[no] allow-vip-to-rport-mapping`

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport-tmplt1
ACOS(config-vport)# allow-vip-to-rport-mapping
```

conn-limit

Description Specifies the maximum number of connections allowed on virtual ports that use this template.

Syntax `[no] conn-limit connections [reset] [no-logging]`

Parameter	Description
connections	Maximum number of concurrent connections, 1-64000000.
reset	Specify the action to take for connections after the connection limit is reached on the virtual port. By default, excess connections are dropped. If you change the action to reset, the connections are reset instead. Excess connections are dropped by default.
no-logging	Disable logging when this feature is enabled.

Default 64000000

Mode SLB virtual-port template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command

output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure a connection limit of 10000 connections, and disable logging:

```
ACOS(config)# slb template virtual-port vport-tmplt1
ACOS(config-vserver)# conn-limit 10000 no-logging
```

conn-rate-limit

Description Limits the rate of new connections the ACOS device is allowed to send to virtual ports that use this template. When a virtual port reaches its connection limit, the ACOS device stops selecting the port for client requests.

Syntax

```
[no] conn-rate-limit connections
[per {100ms | 1sec}] [reset] [no-logging]
```

Parameter	Description
connections	Maximum new connections allowed on a server. You can specify 1-1048575 connections.
per {**100ms** | **1sec**}	Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (1sec).
reset	Send a reset (RST) to a client after the connection rate has been exceeded. By default (without this option), the ACOS device silently drops the request. If you configure a limit for a virtual server and also for an individual port, the ACOS device uses the lower limit.
no-logging	Disable logging when this feature is enabled.

Default Not configured by default.

Mode SLB virtual-port template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-

server template bound to the virtual server or virtual port, the connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure a connection rate limit of 10000 connections per second, and disable logging:

```
ACOS(config)# slb template virtual-port vport-tmply1
ACOS(config-vserver)# conn-rate-limit 10000 no-logging
```

drop-unknown-conn

Description Drop the connection a TCP packet without a SYN or RST flag is received, and the packet does not belong to any existing connections.

Syntax

```
[no] drop-unknown-conn
```

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# drop-unknown-conn
```

dscp

Description Sets the Differentiated Services Code Point (DSCP) value in client requests before forwarding them to the server.

Syntax

```
[no] dscp num
```

Parameter	Description
num	You can set the DSCP value to 1-63.

Mode SLB virtual-port template

Example The following example illustrates how this feature works:

1. Configure a port template named `t1` that marks DSCP 4 on outgoing packets.

```
slb template port t1
  dscp 4
```

2. Configure a virtual-port template named `vp1` that marks DSCP 6 on outgoing packets.

```
slb template virtual-port vp1
  dscp 6
```

3. Bind `t1` to both `port 80 tcp` and `port 443 tcp`.

```
  slb server s1 9.8.8.15
  port 80 tcp
    template port t1
  port 443 tcp
    template port t1
```

4. Configure a virtual server named `vip2` with virtual `port 80 http` and `port 443 tcp`. Although the `vp1` template is bound to both ports, outgoing packets are marked with DSCP 4, because real ports take precedence over virtual ports.

```
  slb virtual-server vip2 fd5a:bfc:563c:bcda::100
  port 80 http
    source-nat pool s2
    service-group sg-80-6
      template virtual-port vp1
  port 443 https
    source-nat pool s2
    service-group sg-443-6
      template server-ssl s1
      template client-ssl cl-ssl1
      template virtual-port vp1
```

ignore-tcp-msl

Description Immediately reuse TCP sockets after session termination, without waiting for the SLB Maximum Session Life (MSL) time to expire.

Syntax

```
[no] ignore-tcp-msl
```

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# ignore-tcp-msl
```

non-syn-initiation

Description Enables a TCP session to be created when the initial TCP packet is non-SYN.

This feature is useful in VRRP-A topologies where, after a failover, a non-SYN packet from the existing connection arrives at the new active device and a session can be created on the new active device without having to configure haconn- mirror under the virtual port.

Syntax

```
[no] non-syn-initiation
```

Default Not enabled.

Mode SLB virtual-port template

Usage To guarantee the same backend server is selected after failover, use the src-ip-only method.

This feature is only supported on TCP virtual ports and not supported when:

- source-nat is configured on the virtual port.
- syn-cookie is configured on the virtual port.
- A conn-limit is configured on a real server or real port

pkt-rate-limit

Description Configure packet rate limit for the virtual port.

Syntax

```
[no] pkt-rate-limit TYPE rate pkt-rate [SAMPLE] [THOLD] [LOG]
[RR]
```

Parameter	Description
TYPE	Specifies the rate limited source. Options include:

Parameter	Description
	• `src-ip-port` — configure source IP and port rate limit. • `src-port` — configure source port limit
`pkt-rate`	Specifies the packet rate (per second). Value range is 1 to 1048575.
`SAMPLE`	Specifies packet rate sampling interval. Options include: • <no parameter> — packet rate sampling is measured in one second intervals. • `per second` — packet rate sampling is measured in one second intervals. • `per 100ms` — packet rate sampling is measured in 100 ms intervals
`THOLD`	Specifies a packet rate threshold for sending a TCP reset that terminates sessions that exceeds the threshold. Options include: • <no parameter> — threshold is not set and TCP reset is never sent. • `reset` *`rst-rate`* — TCP reset is sent when packet rate exceeds rst-rate (range is 1 to 1048575). The reset rate should be greater than the packet rate (pkt-rate).
`LOG`	Specifies event logging frequency when packet rate is exceeded. Options include: • <no parameter> — Log rate is once per minute (default). • `no-logging` — log entries are not created when packet rate limit is exceeded. • `no-repeat-logging` — event is logged once.
`RR`	Specifies use of round robin distribution to trigger rate

Parameter	Description
	limiting. Options include: • <no parameter> — CPU distribution algorithm not considered. • `when-rr-enable` — Packets are rate limited only when CPU round-robin is triggered.

Default Not enabled.

Mode SLB virtual-port template

Example These commands configure a template with a packet rate limit such packets are dropped when the rate from a source port exceeds 500 packets per second; a TCP reset is sent to terminate the session when the source's packet rate exceeds 1000 packets per second.

```
ACOS(config)# slb template virtual-port vsettings
ACOS(config-vport)# pkt-rate-limit src-port rate 500 reset
1000
ACOS(config-vport)#
```

reset-l7-on-failover

Description Resets a Layer 7 connection upon failover.

Syntax

```
[no] reset-l7-on-failover
```

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# reset-l7-on-failover
```

reset-unknown-conn

Description Enables sending TCP Reset (RST) in response to a session mismatch, which occurs when the ACOS device receives a TCP packet for a TCP session that is not in the active session table on the ACOS device.

Syntax `[no] reset-unknown-conn`

Default Not enabled.

Mode SLB virtual-port template

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# reset-unknown-conn
```

snat-msl

Description Set the Maximum Segment Life (MSL) for source-NAT connections. This option is useful for servers that have older TCP/IP stacks, which wait up to 240 seconds (4 minutes) after a FIN before the endpoint can enter a new connection.

Syntax `[no] snat-msl seconds`

Parameter	Description
seconds	You can set the MSL to 1-1800 seconds.

Mode SLB virtual-port template

Example Set the source-NAT MSL to 45 seconds.

```
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# snat-msl 45
```

snat-port-preserve

Description Attempts to preserve the client's source port for traffic destined for the virtual port.

Syntax `[no] snat-port-preserve`

Default Not enabled.

Mode SLB virtual-port template

Usage This feature works on the following two conditions:

- Always attempt snat port preserve: When the configured virtual port matches the configured real port, the show slb l4 respective counters are incremented accordingly. For example,

```
ACOS# show slb l4
Total
-------------------------------------------------------------
-
.....
NAT Port Preserve Try 1
NAT Port Preserve Succ 1
.....
```

- Best Effort: When the hashing of an incoming client source port and configured real port matches the current CPU and when this condition fails, then neither of the above counters will increment.

Limitation

- Port preservation is not always guaranteed and is performed on a best-effort basis.
- Port preservation depends on the number of Platform CPUs. Hence, in some cases, the ports from 1024 - <xxxx> will not be preserved.
- Port preservation does not work for FTP active mode sessions.
- Port preservation works only if source NAT is enabled for the virtual port.

Example Enable this feature:

```
ACOS(config)# slb template virtual-port vport1
ACOS(config-vport)# snat-port-preserve
```

slb template virtual-server

Description Configure a template of SLB settings for virtual servers.

NOTE: Before changing a default template, make sure the changes you plan to make are applicable to all virtual ports that use the template.

Syntax

```
[no] slb template virtual-server {default | template-name}
```

Parameter	Description
default	Edit the default virtual server template. This template can be modified in the same way as any custom *template-name* you specify.
template-name	Template name (1-127 characters)

This command enters the SLB Virtual Server Template Configuration Mode Commands for the specified Virtual-Server template.

Mode Configuration mode

Usage The normal form of this command creates a virtual server template. The **no** form of this command removes the template.

You can bind only one virtual server template to a virtual server. However, you can bind the virtual server template to multiple virtual servers.

Some of the parameters that can be set using a template can also be set or changed on the individual virtual server:

- If a parameter is set (or changed from its default) in both a template and on the individual virtual server, the setting on the individual virtual server takes precedence.
- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual virtual server, the setting in the template takes precedence.

Example The following commands configure a virtual server template called “vs-tmplt1” that sets ICMP rate limiting and bind the template to a virtual server:

```
ACOS(config)# slb template virtual-server vs-tmplt1
ACOS(config-vserver)# icmp-rate-limit 25000 lock 30000 60
ACOS(config-vserver)# exit
ACOS(config)# slb virtual-server vip1 10.10.10.2
ACOS(config-slb virtual server)# template virtual-server vs-tmplt1
```

conn-limit

Description Specifies the maximum number of connections allowed on virtual servers that use this template.

Syntax

```
[no] conn-limit connections [reset] [no-logging]
```

Parameter	Description
connections	Maximum number of concurrent connections, 1-64000000.
reset	Specify the action to take for connections after the connection limit is reached on the virtual server. By default, excess connections are dropped. If you change the action to reset, the connections are reset instead. Excess connections are dropped by default.
no-logging	Disable logging when this feature is enabled.

Default 64000000

Mode SLB virtual-server template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure a connection limit of 10000 connections, and disable logging:

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# conn-limit 10000 no-logging
```

conn-rate-limit

Description Limits the rate of new connections the ACOS device is allowed to send to servers that use this template. When a real server reaches its connection limit, the ACOS device stop selecting the server for client requests.

Syntax

```
[no] conn-rate-limit connections
[per {100ms | 1sec}] [reset] [no-logging]
```

Parameter	Description
connections	Maximum of new connections allowed on a server. You can specify 1-1048575 connections.
per {**100ms** | **1sec**}	Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (1sec).
reset	Send a reset (RST) to a client after the connection rate has been exceeded. By default (without this option), the ACOS device silently drops the request. If you configure a limit for a server and also for an individual port, the ACOS device uses the lower limit.
no-logging	Disable logging when this feature is enabled.

Default Not configured by default.

Mode SLB virtual-server template

Usage If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example Configure a connection rate limit of 10000 connections per second, and disable logging:

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# conn-rate-limit 10000 no-logging
```

disable-when-all-ports-down

Description Disable virtual server when all member ports are down.

Syntax `[no] disable-when-all-ports-down`

Default Not set by default.

Mode SLB virtual-server template

Example To disable when all ports down.

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# disable-when-all-ports-down
ACOS(config-vserver)# no disable-when-all-ports-down
```

disable-when-all-ports-down

Description Disable virtual server when all member ports are down.

Syntax `[no] disable-when-all-ports-down`

Default Not set by default.

Mode SLB virtual-server template

Example To disable when any port down:

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# disable-when-any-port-down
ACOS(config-vserver)# no disable-when-any-port-down
```

icmp-rate-limit

Description Configures ICMP (v4) rate limiting for the virtual server, to protect against denial-of-service (DoS) attacks.

Syntax `[no] icmp-rate-limit normal-rate [lockup max-rate lockup-time]`

Parameter	Description
normal-rate	Maximum number of ICMP packets allowed per second. If the virtual server receives more than the normal rate of ICMP packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.

Parameter	Description
max-rate	Maximum number of ICMP packets allowed per second before the ACOS device locks up ICMP traffic to the virtual server. When ICMP traffic is locked up, all ICMP packets are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the ACOS device drops all ICMP traffic to the virtual server, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

Default By default, this is not set. When enabled, specifying a maximum rate (lockup rate) and lockup time is optional. If you do not specify them, lockup does not occur.

Mode SLB virtual-server template

Example Configure ICMP rate limiting to allow 5000 packets per second.

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# icmp-rate-limit 5000
```

icmpv6-rate-limit

Description Configures ICMPv6 rate limiting for the virtual server, to protect against denial-of-service (DoS) attacks.

Syntax

```
[no] icmpv6-rate-limit normal-rate [lockup  max-rate lockup-time]
```

Parameter	Description
normal-rate	Maximum number of ICMPv6 packets allowed per second. If the virtual server receives more than the normal rate of ICMP packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.

Parameter	Description
max-rate	Maximum number of ICMPv6 packets allowed per second before the ACOS device locks up ICMPv6 traffic to the virtual server. When ICMPv6 traffic is locked up, all ICMPv6 packets are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the ACOS device drops all ICMPv6 traffic to the virtual server, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

Default Not set by default. When enabled, specifying a maximum lockup rate and lockup time is optional. When they are not specified, lockup does not occur.

Mode SLB virtual-server template

Example Configure ICMPv6 rate limiting to allow 5000 packets per second.

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# icmpv6-rate-limit 5000
```

subnet-gratuitous-arp

Description Enables gratuitous ARPs for all VIPs in subnet VIPs. A subnet VIP is a range of VIPs created from a range of IP addresses within a subnet.

This option applies only to VIPs created using a range of subnet IP addresses. The option has no effect on VIPs created with a single IP address.

Syntax

```
[no] subnet-gratuitous-arp
```

Default This is disabled by default; the ACOS device sends gratuitous ARPs for only the first IP address in a subnet VIP.

Mode SLB virtual-server template

Example Send a gratuitous ARPs for every IP in the subnet virtual server.

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# subnet-gratuitous-arp
```

support-http2

Description Enable HTTP/2 support.

Syntax

```
[no] support-http2
```

Default Not enabled.

Mode SLB virtual-server template

Usage This command can be configured in the following ways:

- If configured with source-nat, then ACOS will open multiple server connections for each connected client.
- If configured without source-nat, then ACOS will open only one server connection for each connected client. We support server-side HTTP/2 by mapping one-to-one relationship with the client HTTP/2 connection.

Example The following command configures HTTP/2 with source-nat.

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# source-nat pool snat-pool1
ACOS(config-slb vserver-vport)# support-http2
```

Example The following command configures HTTP/2 without source-nat.

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# support-http2
```

template server-ssl

Description Bind a server-ssl template to the virtual server.

Syntax

```
[no] template server-ssl  template-name
```

Default None

Mode Virtual server

slb transparent-acl-template

Description Set the idle timeout value for ACL-related pass-through TCP sessions.

A pass-through TCP session is one that is not terminated by the ACOS device (for example, a session for which the ACOS device is not serving as a proxy for SLB).

Syntax

```
[no] slb transparent-acl-template template-name
```

Replace *template-name* with the name of an existing TCP template (1-63 characters).

Default The default idle timeout for pass-through TCP sessions is 30 minutes. The default idle timeout in TCP templates is 120 seconds.

Mode Configuration mode

Usage Only the idle timeout setting in the specified TCP template is applicable to pass-through TCP sessions. None of the other options in TCP templates affect pass-through TCP sessions.

The maximum idle timeout supported for transparent sessions is 15300 seconds. This is true even if the idle timeout in the TCP template itself is set to a higher value. Higher idle timeout values apply only to SLB sessions, not to transparent sessions. This is because transparent sessions are stateless and can be recreated if timed out.

Example The following command configures the default TCP template, setting the idle timeout value to 15000 seconds. This template (and thus, idle timeout value) are then applied to ACL-related pass-through TCP sessions:

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# idle-timeout 15000
ACOS(config-l4 tcp)# exit
ACOS(config)# slb transparent-acl-template default
```

Related Commands:

- slb template tcp
- slb transparent-tcp-template

slb transparent-tcp-template

Description Set the idle timeout value for pass-through TCP sessions.

A pass-through TCP session is one that is not terminated by the ACOS device (for example, a session for which the ACOS device is not serving as a proxy for SLB).

Syntax

```
[no] slb transparent-tcp-template template-name
```

Replace *template-name* with the name of an existing TCP template (1-63 characters).

Default The default idle timeout for pass-through TCP sessions is 30 minutes. The default idle timeout in TCP templates is 120 seconds.

Mode Configuration mode

Usage Only the idle timeout setting in the specified TCP template is applicable to pass-through TCP sessions. None of the other options in TCP templates affect pass-through TCP sessions.

The maximum idle timeout supported for transparent sessions is 15300 seconds. This is true even if the idle timeout in the TCP template itself is set to a higher value. Higher idle timeout values apply only to SLB sessions, not to transparent sessions. This is because transparent sessions are stateless and can be recreated if timed out.

Example The following command configures the default TCP template, setting the idle timeout value to 15000 seconds. This template (and thus, idle timeout value) are then applied to pass-through TCP sessions:

```
ACOS(config)# slb template tcp default
ACOS(config-l4 tcp)# idle-timeout 15000
ACOS(config-l4 tcp)# exit
ACOS(config)# slb transparent-tcp-template default
```

Related Commands:

- slb template tcp
- slb transparent-acl-template

slb virtual-server

Description Configure a virtual server.

Syntax

```
[no] slb virtual-server name
  [use-if-ip {ethernet num | loopback num}] |
  [ipv6-addr [ipv6-acl acl-name]] |
  [ipv4-addr [/mask-length | subnet-mask] acl acl-name]
  [substitute-source-mac [ignore-global]]
 [gtp-session-lb]
```

The “no” form of this command deletes the specified virtual server. If the **delete-referenced-tagged-objects** option of system config-mgmt is enabled (the default setting), the system deletes the service group regardless of any existing references. If this option is disabled, the system checks if the virtual server is being referenced by other objects and prevents deletion until all references are manually removed.

Parameter	Description
name	Virtual server name, 1-127 characters. If you want to rename the server name, then use **rename** global configuration command.
use-if-ip	Use the IP address of the specified interface. This option is used on vThunder systems only.
ipv6-addr	IPv6 address of the virtual server. If you are configuring an IPv6 wildcard VIP, enter `::` as the IP address. Use the **acl** *acl-id* option to specify IP addresses to be handled as wildcard VIPs. (For more information, see the “Wildcard VIPs” chapter in the *Application Delivery* **Controller** *Guide*.) After you have created a virtual server, you can use this command to change the IP address associated with this name.
ipv4-addr	IPv4 address of the virtual server.

Parameter	Description
	If you are configuring a wildcard VIP, enter `0.0.0.0` as the IP address. Use the **`acl`** *`acl-id`* option to specify IP addresses to be handled as wildcard VIPs. (For more information, see "Wildcard VIPs" chapter in the *Application Delivery* **Controller** *Guide*.) After you have created a virtual server, you can use this command to change the IP address associated with this name. To configure a contiguous set of IPv4 VIPs, specify the subnet mask or mask length. The specified *`ipv4-addr`* will be the starting IP address of this set of VIPs.
substitute-source-mac	Replaces the client (source) MAC address of the packet sent to the load balancing server with the MAC address of the outgoing interface (for example, an AX). This allows real servers in a load balancing environment to make *web cache* or *security device* responses to the source MAC of the ACOS device. Use the `ignore-global` option to ignore the global setting and prevent the virtual port from changing the source MAC address.
gtp-session-lb	Configure GTP session load balancing for SLB virtual server. Enables the stateful parsing of GTP payload to ensure that multiple requests on the same 5-tuple can be correctly load balanced to different virtual servers.

Default N/A

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing virtual server and related load balancing configurations and

parameters. The CLI changes to the configuration level for the virtual server.

The “no” form of this command removes an existing virtual server.

The maximum number of virtual servers is configurable. See slb resource-usage.

Notes on VIP Ranges

- The IP addresses in the specified subnet range can not belong to an IP interface, real server, or other virtual server configured on the ACOS device.
- The largest supported IPv4 subnet length is /16.
- Statistics are aggregated for all VIPs in the subnet virtual server.
- The current release supports this feature only for DNS ports on the default DNS port number (TCP port 53 or UDP port 53).

Example The following commands configure a new virtual server named “vs1” and associate virtual ports, service group, and enable GTP sessions for server load balancing.

```
ACOS(config)# slb virtual-server vs1 10.10.2.1
ACOS(config-slb vserver)# port 2123 udp
ACOS(config-slb vserver: vport)# service-group sg1
ACOS(config-slb vserver: svcgrp)# gtp-session-lb
```

template client-ssl

Description Bind a client-ssl template to the virtual port.

Syntax

```
[no] template client-ssl template-name
```

Default None

Mode Virtual port

Example This following example applies to bind an existing client-ssl template to a virtual port. In this case, the TLS service is provided to the corresponding endpoint:

```
ACOS(config-slb vserver-vport)# port 53 dns
ACOS(config-slb vserver-vport)# template client_SSL
```

template server

Description Bind a real server template to the server.

Syntax

```
[no] template server template-name
```

Default The real server template named “default” is bound to servers by default. The parameter settings in the default real server template are automatically applied to the new server, unless you bind a different real server template to the server.

Mode Real server

Usage If a parameter is set individually on this server and also is set in a server template bound to this server, the individual setting on this server is used instead of the setting in the template.

To configure a real server template, see slb template server.

Example The following commands configure a real server template called “rs-tmplt1” and bind the template to two real servers:

```
ACOS(config)# slb template server rs-tmplt1
ACOS(config-rserver)# health-check ping2
ACOS(config-rserver)# conn-limit 500000
ACOS(config-rserver)# exit
ACOS(config)# slb server rs1 10.1.1.99
ACOS(config-real server)# template server rs-tmplt1
ACOS(config-real server)# exit
ACOS(config)# slb server rs2 10.1.1.100
ACOS(config-real server)# template server rs-tmplt1
```

arp-disable

Description Disable ARP replies from a virtual server.

Syntax

```
[no] arp-disable
```

Default ARP replies are enabled by default.

Mode Virtual server

Usage Use this command if you do not want the ACOS device to reply to ARP requests to the virtual server's IP address. For example, you can use this command to put a VIP out of service on one ACOS device and use that device as a switch or router for another ACOS device providing SLB for the VIP.

When you disable ARP replies for a VIP, redistribution of routes to the VIP is automatically disabled.

Example The following command disables ARP replies:

```
ACOS(config-slb vserver)# arp-disable
```

description

Description Add a description to a VIP.

Syntax

```
description string
```

Replace *string* with a description of the VIP (up to 63 characters long). The string can contain blanks. Quotation marks are *not* required.

Default None

Mode Virtual server

disable

Description Disable a virtual server.

Syntax

```
[no] disable
```

Default Virtual servers are enabled by default.

Mode Virtual server

disable-when-all-ports-down

Description Automatically disable the virtual server if *all* its service ports are down. If OSPF redistribution of the VIP is enabled, the ACOS device also withdraws the route to the VIP in addition to disabling the virtual server.

Syntax

```
[no] disable-when-all-ports-down
```

OR

Syntax

```
[no] disable-when-any-ports-down
```

Parameter	Description
when-all-ports-down	Automatically disables the virtual server if *all* its service ports are down. If OSPF redistribution of the VIP is enabled, the ACOS device also withdraws the route to the VIP in addition to disabling the virtual server.
when-any-port-down	Automatically disables the virtual server if *any* of its service ports is down. If OSPF redistribution of the VIP is enabled, the ACOS device also withdraws the route to the VIP in addition to disabling the virtual server.

Default Enabled.

Mode Virtual server

disable-when-any-port-down

Description Automatically disable the virtual server if any of its service ports is down. If OSPF redistribution of the VIP is enabled, the ACOS device also withdraws the route to the VIP in addition to disabling the virtual server.

Syntax

```
[no] disable-when-any-port-down
```

Default Disabled.

Mode SLB Virtual-server template

Example To disable when any port down.

```
ACOS(config)# slb template virtual-server vstempl1
ACOS(config-vserver)# disable-when-any-port-down
```

enable

Description Enable a virtual server.

Syntax

```
[no] enable
```

Default Enabled

Mode Virtual server

Example The following commands re-enable virtual server “vs1”:

```
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# enable
```

extended-stats

Description Enable collection of peak connection statistics for a virtual server.

Syntax

```
[no] extended-stats
```

Default Disabled

Mode Virtual server

port

Description Configure a virtual port on a virtual server.

Syntax

```
[no] port port-number service-type [range length] [alternate]
```

Parameter	Description
port	Port number, 0-65534.
service-type	Service type of the port: • `diameter` – Diameter AAA load balancing

Parameter	Description
	• `dns-tcp` – DNS service over TCP • `dns-udp` – DNS caching • `fast-http` – Streamlined Hypertext Transfer Protocol (HTTP) service • `fix` – File Information Exchange (FIX) load balancing • `ftp` – File Transfer Protocol • `ftp-proxy` – FTP proxy service • `http` – HTTP • `https` – Secure HTTP (SSL) • `imap` - Internet Message Access Protocol • `mlb` – MLB service over TCP • `mms` – Microsoft Media Server • `mqtt` – MQ Telemetry Transport protocol. A lightweight publish-subscribe protocol . • `mqtts` – MQ Telemetry Transport protocol for secured communication. • `mssql` – Database load balancing for MS-SQL servers • `mysql` – Database load balancing for MySQL servers • `quic`- Quick UDP Internet Connections. This port should be used when you want to process QUIC layer traffic. **NOTE:** QUIC configuration is supported only with the TLS 1.3 SSL Library. • `http-over-quic` – HTTP/3 over QUIC. This port

Parameter	Description
	should be used when you want to process HTTP/3 traffic.
service-type (continued)	• `others` – Wildcard port used for IP protocol load balancing. For more information, see"IP Protocol Load Balancing" in Application Delivery Controller Guide. • **`pop3`** - (Post Office Protocol 3) • `radius` – RADIUS • **`reqmod-icap`** - ICAP • **`respmod-icap`** - ICAP • `rtsp` – Real Time Streaming Protocol • `sip` – Session Initiation Protocol (SIP) over UDP • `sip-tcp` – SIP over TCP • `sips` – SIP over TCP / TLS • `smpp-tcp` – Short Message Peer-to-Peer (SMPP 3.3) load balancing over TCP • `smtp` – Simple Mail Transfer Protocol • `spdy` – Google SPeeDy protocol • `spdys` – Secure SPDY • `ssl-proxy` – SSL proxy service • `ssli` – non-HTTP over SSL • `tcp` – Layer 4 Transmission Control Protocol (TCP) • `tcp-proxy` – Full TCP-stack service for load-balanced Layer 7 applications • `tftp` – Trivial File Transfer Protocol • `udp` – User Datagram Protocol
`range` *length*	Assigns a range of ports to the VIP for the specified virtual-service type. The length specifies the number

Parameter	Description
	of contiguous ports to add to the base port, 0-254.
`alternate`	Designates this virtual port as an alternate port for another virtual port. An alternate port is a standby for the primary port. (See alternate.)

Default N/A

Mode Virtual server

Usage The normal form of this command creates a new or edits an existing virtual port. The CLI changes to the configuration level for the virtual port.

The “no” form of this command removes the specified virtual port from current virtual server.

The maximum number of virtual service ports allowed and the maximum number per virtual server depend on the ACOS model.

The ACOS device allocates processing resources to HTTPS virtual ports when you bind them to an SSL template. This results in increased CPU utilization, regardless of whether traffic is active on the virtual port.

Fast-HTTP

Fast-HTTP is optimized for very high performance information transfer in comparison to regular HTTP. Due to this optimization, fast-HTTP does not support all the comprehensive capabilities of HTTP such as header insertion and manipulation. It is recommended not to use fast-HTTP for applications that require complete data transfer integrity.

Packet Processing on HTTP Virtual Ports

Packets reaching a Layer 7 HTT{P virtual port are processed in the following order of priority:

1. PBSLB (policy template) action drop/reset
2. PBSLB action service-group, in conjunction with PBSLB action.
3. Source-IP persistence template
4. Layer 4 aFleX policy (for example, CLIENT_ACCEPTED event)

5. Cookie persistence template
6. Layer 7 aFleX script (for example, HTTP_REQUEST event)
7. URL switching configured in HTTP template
8. Cookie persistence template with match-type of service-group and bound to a source-IP persistence template with match-type set to service-group.
9. Configured service- group bound to the virtual port

Example The following example creates a new (or edits an existing) virtual port:

```
ACOS(config-slb vserver)# port 443 https
ACOS(config-slb vserver-vport)#
```

redistribution-flagged

Description Flag this VIP to selectively enable or disable redistribution of it by OSPF.

Syntax

```
[no] redistribution-flagged
```

Default Not set. VIP is automatically redistributed if VIP redistribution is enabled in OSPF.

Mode Virtual server

Usage Use this option if you want to redistribute only some of the VIPs rather than all of them.

Selective VIP redistribution also requires configuration in OSPF. See the description of the **vip** option of the **redistribute** command.

stats-data-disable

Description Disable collection of statistical data for the virtual server.

Syntax

```
stats-data-disable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual server

stats-data-enable

Description Enable collection of statistical data for the virtual server.

Syntax

```
stats-data-enable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual server

Usage To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally. (See slb common.)

template logging

Description Bind a logging template to the virtual server.

Syntax

```
[no] template logging template-name
```

Default None

Mode Virtual server

template policy

Description Bind a PBSLB policy template to the virtual server.

Syntax

```
[no] template policy  template-name
```

Default None

Mode Virtual server

Usage This command is applicable only for PBSLB policy templates configured for IP limiting. For more information, see *Application Access Management and DDoS Mitigation Guide*.

template scaleout

Description Bind a Scale Out template to the virtual server.

More information about Scale Out is available in “Configuring Scale Out” in the *System Configuration and Administration Guide*.

Syntax `[no] template scaleout template-name`

Default None

Mode Virtual server

template virtual-server

Description Bind a virtual server template to the virtual server.

Syntax `[no] template virtual-server template-name`

Default The virtual server template named “default” is bound to virtual servers by default. The parameter settings in the default virtual server template are automatically applied to the new virtual server, unless you bind a different virtual server template to the virtual server.

Mode Virtual server

Usage If a parameter is set individually on this virtual server and also is set in a virtual server template bound to this virtual server, the individual setting on this virtual server is used instead of the setting in the template.

To configure a virtual server template, see slb template virtual-server.

Example The following commands configure a virtual server template called “vs-tmplt1” that sets ICMP rate limiting, and bind the template to a virtual server:

```
ACOS(config)# slb template virtual-server vs-tmplt1
ACOS(config-vserver)# icmp-rate-limit 25000 lock 30000 60
ACOS(config-vserver)# exit
ACOS(config)# slb virtual-server vip1 10.10.10.2
ACOS(config-slb vserver)# template virtual-server vs-tmplt1
```

vrid

Description Assign the virtual server to a VRRP-A VRID.

Syntax `[no] vrid num`

Use *num* to specify the VRID (1-31 in the shared partition, or 1-7 in an L3V partition).

Default The default VRID, if none is assigned, is 0.

Mode Virtual server configuration mode

slb virtual-server port

To access this configuration level, enter the **port** command at the configuration level for a virtual server.

```
ACOS(config)# slb virtual-server VIP1 192.168.22.22
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)#
```

aflex-table-entry-sync

Description Configure fast aFlex table synchronization to a virtual port. These aFlex tables will be synchronized with ACOS device via VRRP-A.

Syntax

```
[no] aflex-table-entry-sync {enable | disable}
```

Parameter	Description
enable	Enable fast aFlex table synchronization for the defined virtual port.
disable	Disable fast aFlex table synchronization for the defined virtual port.

Default Disabled

Mode Virtual port configuration mode

Example This following command configures aFlex table entry synchronization.

```
ACOS(config)# slb virtual-server vslb1
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# aflex-table-entry-sync enable
```

attack-detection

Description Enable analytics and attack detection using ZBAR. This command helps in identifying volumetric and IOT DDoS attacks on the SLB virtual port and employs mitigation policies to provide excellent application responsiveness for the good actors. The bad sources are dropped or rate-limited based on their computed threat score.

Syntax `[no] attack-detection`

Default N/A

Mode Virtual port

Example The following command enables attack detection on the virtual port:

```
ACOS (config)# slb virtual-server vip1 12.12.12.203
ACOS (config-slb vserver)#  port 80 tcp
ACOS (config-slb vserver-vport)#  attack-detection
```

aaa-policy

Description Bind an AAM policy to the virtual port.

Syntax `[no] aaa-policy policy-name`

Mode Virtual port

access-list

Description Apply an Access Control List (ACL) to a virtual server port.

Syntax

```
[no] access-list {acl-num | name acl-name}
     [source-nat-pool {pool-name | pool-group-name}
        [sequence-number num]]
```

Parameter	Description
acl-num | *name acl-name*	Number of a configured IPv4 ACL (*acl-num*), or the name of a configured IPv6 ACL (**name** *acl-name*).
source-nat-pool {*pool-name* | *pool-group-name*} [**sequence-number** *num*]	Name of a configured IP source NAT pool or pool group. Use this option to configure a policy-based source NAT. Source NAT is required if the real servers are in a different subnet than the VIP. The **sequence-number** option specifies the ACL position within the ACL sequence associated with IP source NAT pools and are assigned to this virtual port. The sequence number is important because the ACOS

Parameter	Description
	device uses IP addresses in the pool associated with the first ACL matching the traffic. By default, the ACL sequence is based on the order in which you apply them to the virtual port. The first ACL has sequence number 1, the second ACL has sequence number 2, and so on. You can specify 1-32 as the sequence number. To view the sequence, use the **show running-config** command to view the configuration for this virtual port.

Default N/A

Mode Virtual port

Usage The ACL must be configured before you can apply it to a virtual port. To configure an ACL, use the "access-list (standard)" or "access-list (extended)" commands, which are described in the "Command Line Interface Reference" document.

To permit or deny traffic on the virtual port, specify an ACL but do not specify a NAT pool.

To configure policy-based source NAT, specify an ACL *and* a NAT pool. Use an extended ACL. The source IP address must match on the client address. The destination IP address must match on the real server address. The action must be permit. The NAT pool is used only for traffic that matches the ACL. This configuration allows the virtual port to have multiple pools, and to select a pool based on the traffic.

Example The following commands configure a standard ACL to deny traffic from subnet 10.10.10.x, and apply the ACL to the inbound traffic direction on virtual port 8080 on virtual server "slb1":

```
ACOS(config)# access-list 99 deny 10.10.10.0 0.0.0.255
ACOS(config)# slb virtual-server vslb1
ACOS(config-slb vserver)# port 8080 http
ACOS(config-slb vserver-vport)# access-list 99
```

Example The following commands configure policy-based source NAT, by binding ACLs to NAT pools on the virtual port.

```
ACOS(config)# slb virtual-server vs1 10.10.10.100
ACOS(config-slb virtual server)# port 80 tcp
ACOS(config-slb vserver-vport)# access-list 30 source-nat-pool
pool1
ACOS(config-slb vserver-vport)# access-list 50 source-nat-pool
pool2
```

aflex

Description Apply an aFleX policy to a virtual port.

Syntax

```
[no] aflex policy-name
```

Replace *policy-name* with the name of a configured aFleX policy.

Default N/A

Mode Virtual port

Usage The normal form of this command applies the specified aFleX policy to the port. The **no** form of this command removes the aFleX policy from the port. For more information about aFleX policies, see the *aFleX Scripting Language Reference*.

Example The following command applies aFleX policy “aflex1” to a virtual port:

```
ACOS(config-slb vserver-vport)# aflex aflex1
```

alternate

Description Enables switchover to another virtual port, based on specific conditions.

Syntax

```
[no] alternate port port-num
{alt-port-service-type [switchover-event]}
```

Parameter	Description
port-num	Port number of the alternate virtual port.
alt-port-	Service type of the alternate port, **tcp** or **http**.

Parameter	Description
service-type	
switchover-event	The event types that cause switchover from the primary port to the alternate port: For TCP alternate ports, you can specify the following: • **req-fail** – Switches over if a request fails. • **when-down** – Switches over if the service group for the primary port is down. • For HTTP alternate ports, you can specify the following: • **serv-sel-fail** – Switches over if SLB server selection fails. • **when-down** – Switches over if the service group for the primary port is down.

Default Not set

Mode Virtual port

bucket-count

Description Configure the number of traffic buckets used in a Scale Out configuration.

Syntax

```
[no] bucket-count num
```

Replace *num* with the number of traffic buckets (1-256).

Mode Virtual port

clientip-sticky-nat

Description Enables sticky-NAT to use the same source NAT IP address for a given client.

Syntax

```
[no] clientip-sticky-nat
```

Default Disabled

Mode Virtual port

Usage You can enable the **clientip-sticky-nat** feature on the individual virtual ports.

This option is not supported with the **ip-rr** (IP round-robin) and **source-nat auto** (smart NAT) options.

Example The following example configures the **clientip-sticky-nat** option:

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# clientip-sticky-nat
```

conn-limit

Description Set the connection limit for a virtual port.

Syntax `[no] conn-limit number [reset] [no-logging]`

Parameter	Description
number	Connection limit, 1-64000000 (64 million).
reset	Sends a connection reset to the client, if the connection limit is reached. If you omit this option, the connection silently drops and no reset is sent to the client.
no-logging	Disables logging for this feature.

Default 64000000

Mode Virtual port

Usage The normal form of this command changes the current port's connection limit. The **no** form of this command resets the port connection limit to its default value.

The connection limit puts a hard limit on the number of concurrent connections supported by the port. No more connections will be put on

the port if its number of current connections is already equal to or bigger than the limit.

- If you set a limit, the default action for any new connection request after the limit has been reached is to silently drop the connection, without sending a reset to the client. Logging is enabled by default.
- If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example The following command changes a virtual port's connection limit to 10000:

```
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# conn-limit 10000
```

def-selection-if-pref-failed

Description Configure SLB to continue checking for an available server in other service groups if all of the servers are down in the first service group selected by SLB.

Syntax

```
def-selection-if-pref-failed
```

Default Enabled

Mode Virtual port

Usage During SLB selection of the preferred server to use for a client request, SLB checks the following configuration areas, in the order listed:

1. Layer 3-4 configuration items:
   - aFleX policies triggered by Layer 4 events

- Policy-based SLB (black/white lists). PBSLB is a Layer 3 configuration item because it matches on IP addresses in black/white lists.

2. Layer 7 configuration items:
   - Cookie switching
   - aFleX policies triggered by Layer 7 events
   - URL switching
   - Host switching
3. Default service group. If none of the items above results in selection of a server, the default service group is used.
   - In single service group configurations, this is the default service group.
   - If the configuration uses multiple service groups, the default service group is the one that is used if none of the templates used by the configuration selects another service group instead.

For example, if an CLIENT_ACCEPTED event triggers an aFleX policy, the policy is consulted first. If an HTTP_REQUEST event triggers an aFleX policy, the policy is consulted if none of the Layer 4 configuration items results in a server selection.

The first configuration area that matches the client or VIP (as applicable) is used, and the client request is sent to a server in the service group that is applicable to that configuration area. For example, if the client's IP address is in a black/white list, the service group specified by the list is used for the client request.

When the def-selection-if-pref-failed option is enabled, SLB continues to check for an available server in other service groups if all servers are down in the first service group selected by SLB.

If Policy-Based SLB (PBSLB) is configured on the same virtual port, PBSLB server-selection failures are not logged. This limitation does not affect failures caused when a client is over itsr PBSLB connection limit. These failures are still logged.

Example The following command enables this option:

```
ACOS(config-slb vserver-vport)# def-selection-if-pref-failed
```

def-selection-if-pref-failed-disable

Description Disable the def-selection-if-pref-failed option. (See “def-selection-if-pref-failed” on page 1.)

Syntax

```
def-selection-if-pref-failed-disable
```

disable

Description Disable a virtual port.

Syntax

```
[no] disable
```

Default Enabled

Mode Virtual port

Example The following command disables a virtual port:

```
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# disable
```

enable

Description Enable a virtual port.

Syntax

```
[no] enable
```

Default Enabled

Mode Virtual port

Example The following command re-enables a virtual port:

```
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# enable
```

extended-stats

Description Enable collection of peak connection statistics for a virtual port.

Syntax

```
[no] extended-stats
```

Default Disabled

Mode Virtual port

force-routing-mode

Description Disables destination NAT, so that server responses go directly to clients.

Syntax

```
[no] force-routing-mode
```

Default Disabled

Mode Virtual port

For IPv4 VIPs, DSR is supported on virtual port (service) types TCP, UDP, FTP, and RTSP. For IPv6 VIPs, DSR is supported on virtual port types TCP, UDP, and RTSP.

gslb-enable

Description Enables Global Server Load Balancing.

Syntax

```
[no] gslb-enable
```

Default Disabled

Mode Virtual port

Example The following command enables Global Server Load Balancing on the virtual port.

```
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# port 53 dns-udp
ACOS(config-slb vserver-vport)# gslb-enable
```

ha-conn-mirror

Description Enable connection mirroring (session synchronization) for the virtual port.

Syntax

```
[no] ha-conn-mirror [on-syn]
```

Parameter	Description
on-syn	Specifies condition that triggers session synchronization. By default the command causes sessions to synchronize when they are is established. When the on-syn parameter is specified, the session synchronizes when the virtual port receives an SYN packet.

Default Disabled.

Mode Virtual port

Usage Connection mirroring applies to VRRP-A configurations. When connection mirroring is enabled, the Active ACOS device sends information about active client connections to the Standby ACOS device. If a failover occurs, the newly Active ACOS device continues service for the session. The client perceives very brief or no interruption.

When connection mirroring is disabled, client session information is lost. Clients must establish new connections.

In VRRP-A deployments, session synchronization is required for persistent sessions (for example, source-IP persistence), and is therefore automatically enabled for these sessions by the ACOS device. Persistent sessions are synchronized even if session synchronization is disabled in the configuration.

Session synchronization applies only to certain virtual port types. The **ha-conn-mirror** command is listed in the CLI help only for those virtual port types.

ipinip

Description Enables IP-in-IP tunneling. This option is available only on the following port types: TCP, UDP, RSTP, FTP, MMS, SIP, TFTP and Radius.

Syntax

```
[no] ipinip
```

Mode Virtual port

ip-map-list

Description Applies an IP map list to the virtual port.

Syntax

```
[no] ip-map-list list-name
```

Default Not set

Mode Virtual port

message-switching

Description Enable message switching.

This causes messages to be forwarded in their entirety, one hop at a time. Each message is treated as its own individual entity.

Syntax

```
[no] message-switching
```

Mode Virtual port

name

Description Change the name assigned to the virtual port.

Syntax

```
name string
```

Replace *string* with the name for the virtual port.

Default The ACOS device assigns a name that uses the following format:

_vip-addr_service-type_portnum

Mode Virtual port

no-auto-up-on-aflex

Description Disable automatic setting of an aFleX-bound virtual port's state to Up.

Syntax

```
[no] no-auto-up-on-aflex
```

Default Disabled. If an aFleX script is bound to the virtual port, the port is automatically marked Up.

Mode Virtual port

Usage This command applies only if an aFleX script is bound to the virtual port.

no-dest-nat

Description Disable destination NAT.

Syntax

```
[no] no-dest-nat [port-translation]
```

For wildcard VIPs, the port-translation option enables the ACOS device to translate the destination protocol port in a client request before sending the request to a server.

This option is useful if the real port number on the server is different from the virtual port number of the VIP. Without this option, the ACOS device sends the request to the server without changing the destination port number.

This option does not change the destination IP address of the request.

This option is supported only for virtual ports that are on wildcard VIPs.

Default Destination NAT is enabled by default.

Mode Virtual port

Usage This option can be used for Direct Server Return (DSR) or for wildcard VIPs.

Direct Server Return

For virtual servers that have a specific virtual IP address (VIP), disabling destination NAT enables Direct Server Return (DSR). When DSR is enabled, only the destination MAC address is translated from the VIP's MAC address to the real server's MAC address. The destination IP address is still the VIP.

In DSR topologies, reply traffic from the server to the client is expected to bypass the ACOS device.

In the current release, for IPv4 VIPs, DSR is supported on virtual port types (service types) TCP, UDP, FTP, and RTSP. For IPv6 VIPs, DSR is supported on virtual port types TCP, UDP, and RTSP.

Wildcard VIPs

For wildcard VIPs (VIPs that can have any IP address), this option enables the ACOS device to send the client request to the server without changing the destination IP address of the request.

The destination port of the request also is unchanged, *unless* you use the **port-translation** option. (See above.)

Depending on the network topology and the application, reply traffic from the server to the client may or may not pass back through the ACOS device. If the **port-translation** option is used, and reply traffic passes through the ACOS device, the ACOS device translates the source port of the server reply back into the destination port to which the client sent the request, before forwarding the reply to the client.

The **port-translation** option is supported only for the following virtual port types: TCP, UDP, and HTTP/HTTPS.

optimization-level

Description Set the HTTP optimization level.

Syntax

```
[no] optimization-level
```

Parameter	Description
0	No optimization
1	Optimization level 1 ACOS optimizes the HTTP code path, which reduces the processing time in the TCP stack as well as the HTTP processing.

Default 0 (No optimization)

Mode Virtual port

Usage

When configuring **optimization-level 1**, ACOS dynamically determines if it can process the HTTP traffic using the optimized code path. If it cannot optimize traffic, it will use the default behavior of **optimization-level 0**.

Certain types of traffic and configurations will not use an optimized code path and, instead, will default to a non-optimized path. They include:

- AAM
- aFleX
- Compression
- External service
- HA failover
- HTTP 1.0 traffic
- HTTP/2 traffic
- HTTP redirect
- HTTP retry
- HTTP policy template
- ICAP
- IP fragmentation
- Jumbo frames
- Policy-based load balancing
- RAM cache
- Scaleout
- SSL
- TCP-proxy templates
- Virtual-port templates
- WAF

Example

This command configures an HTTP port to improve the performance for HTTP traffic.

```
ACOS(config)# slb virtual-server vip2 1.1.1.101
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# optimization-level 1
```

rate-limit-pr-log

Description For Thunder integrations with the A10 Lightning Controller, this commands configures the rate limit for Per Request logging. This is used to prevent the Thunder devices from sending too many log messages to the Lightning Controller at a rate that would exceed the capability of the controller to accept them.

Syntax

```
[no] rate-limit-pr-log num
```

Default Disabled

Mode Virtual port

Usage This command is only available on HTTP virtual ports.

redirect-fwd

Description In a single partition SSLi deployment, the forward direction steers layer 2 traffic from client to Internet on the specified interface.

Syntax

```
[no] redirect-fwd {ethernet eth-id | trunk trunk-id}
```

Default Disabled

Mode Virtual port

Example The following example shows using the `redirect-fwd` command to select the forward direction for steering the layer 2 traffic from the client destined for a traffic inspection device out Ethernet 3.

```
ACOS(config)# slb virtual-server inside1 0.0.0.0 acl 102
ACOS(config-slb vserver)# port 0 tcp
ACOS(config-slb vserver-vport)# service-group sg_real_server_
tcp
ACOS(config-slb vserver-vport)# no-dest-nat
ACOS(config-slb vserver-vport)# redirect-fwd ethernet 3
ACOS(config-slb vserver-vport)# exit
```

redirect-rev

Description In a single partition SSLi deployment, the reverse direction steers layer 2 traffic from Internet to client on the specified interface.

Syntax `[no] redirect-rev {ethernet eth-id | trunk trunk-id}`

Default Disabled

Mode Virtual port

Usage This is only supported under the wildcard VIP 0.0.0.0 for SSLi..

Example The following example shows the `redirect-rev` command to select the reverse direction for steering the layer 2 traffic destined for the security device from the Internet out Ethernet 5.

```
ACOS(config)# slb virtual-server outside1 0.0.0.0 acl 103
ACOS(config-slb vserver)# port 0 tcp
ACOS(config-slb vserver-vport)# service-group sg_real_server_
tcp
ACOS(config-slb vserver-vport)# no-dest-nat
ACOS(config-slb vserver-vport)# redirect-rev ethernet 5
ACOS(config-slb vserver-vport)# exit
```

redirect-to-https

Description Responds to client HTTP requests with an HTTP redirect response with response code 302 (Moved Permanently). The client is redirected to the same host and URI they requested, but using HTTPS instead of HTTP.

Syntax `[no] redirect-to-https`

Default Disabled

Mode Virtual port

Usage This command is only available on HTTP virtual ports.

reply-acme-challenge

Description Enable reply ACME http-01 challenge for CA server. The challenge from CA server goes into data port. This option only takes effect in HTTP port 80 and works on both old and new proxy.

Since the CA server verifies whether the ACME client controls the domain, on the ACOS side, the user must manually configure reverse

proxy. The domain to be verified is the certificate's Common Name. For DNS mapping, the domain's IP address is ACOS's virtual IP address.

NOTE: If one domain maps to multiple IP addresses, then you must configure multiple VIPs, and enable this option on all the HTTP virtual ports.

Syntax `[no] reply-acme-challenge`

Default Disabled

Mode Virtual port

Usage This command is only available on HTTP virtual ports.

Example The following command enables this option.

```
ACOS (config)# slb virtual-server VIP1 192.168.22.22
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# reply-acme-challenge
```

reset-on-server-selection-fail

Description Send a TCP reset (RST) to the client if server selection fails.

Syntax `[no] reset-on-server-selection-fail`

Default Disabled

Mode Virtual port

Usage The TCP template **reset-rev** option also can be used to send a RST to clients. In prior releases, the **reset-rev** option would send a RST in response to a server selection failure. However, this is no longer true. The **reset-on-server-selection-fail** option must be used instead.

rtp-sip-call-id-match

Description Causes RTP traffic try to match the real server of an SIP SMP call-id session.

This command is used in conjunction with the **smp-call-id-rtp-session** option under slb template sip (over UDP), which creates a cross-CPU RTP session that can be matched by RTP traffic.

Syntax `[no] rtp-sip-call-id-match`

Mode Virtual port

Example The example below shows a sample configuration:

```
!
slb template sip test
   smp-call-id-rtp-session
!
!
slb virtual-server vv 0.0.0.0
   port 0 udp
      skip-rev-hash
      message-switching
      force-routing-mode
      no-dest-nat
      service-group win
      rtp-sip-call-id-match
   port 5060 sip
      message-switching
      force-routing-mode
      service-group winms
      template sip test
!
```

service-group

Description Bind a virtual port to a service group.

Syntax `[no] service-group group-name`

Replace *group-name* with the service-group name.

Default N/A

Mode Virtual port

Usage The normal form of this command binds the virtual port to the specified service group. The “no” form of this command removes the binding.

One virtual port can be associated with one service group only, while one service group can be associated with multiple virtual ports. The

type of service group and type of virtual port should match. For example, a UDP service group can not be bound to an HTTP virtual port.

Example The following command binds DNS-UDP group-name with DNS-UDP port.

```
ACOS(config-slb vserver-vport)# port 52 dns-udp
ACOS(config-slb vserver-vport)# source-nat auto
ACOS(config-slb vserver-vport)# service-group dns-udp
```

skip-rev-hash

Description Will not insert reverse tuple into the hash for lookup. This is used with aFlex with stateless load-balancing methods.

Syntax

```
[no] skip-rev-hash
```

Mode Virtual port

Example The following example shows how to activate this feature.

```
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# skip-rev-hash
```

snat-on-vip

Description Enable IP NAT support for the virtual port.

Syntax

```
[no] snat-on-vip
```

Default Disabled

Mode Virtual port

Usage Source IP NAT can be configured on a virtual port in the following ways:

1. ACL-based source NAT (**access-list** command at virtual port level)
2. VIP source NAT (**slb snat-on-vip** command at global configuration level)
3. aFleX policy (**aflex** command at virtual port level)
4. Non-ACL source NAT (**source-nat** command at virtual port level)

These methods are used in the order shown above. For example, if IP source NAT is configured using an ACL on the virtual port, and the **slb snat-on-vip** command is also used, then a pool assigned by the ACL is used for traffic that is permitted by the ACL. For traffic that is not permitted by the ACL, VIP source NAT can be used instead.

The device does not support source IP NAT on FTP or RTSP virtual ports.

source-nat auto

Description Configure Smart NAT, to automatically create NAT mappings using the ACOS interface connected to the real server.

Syntax

```
[no] source-nat auto {precedence | ip-rr}
```

Parameter	Description
precedence	Set the auto NAT pool as higher precedence for source NAT. This option is applicable if standard NAT pools are also used by the virtual port. In this case, using this option causes Smart NAT to be used before the standard NAT pools are used.
ip-rr	Enable the IP address round-robin method for source NAT. This option is applicable if you want to round-robin across multiple floating IPs for VRRP-A or interface IPs without VRRP-A to reach more than 41K. The IP addresses rotates through the floating or interface IPs for every request to balance out the traffic across all the IPs.

Default Disabled

Mode Virtual port

Usage If you do not use VRRP-A, 41K ports per interface IP address are used for Smart NAT mappings. ACOS can use the same ACOS interface IP

address and port for more than one server connection. The combination of ACOS IP address and port number (source) and server IP address and port (destination) uniquely identifies each mapping.

Additional Notes

- Smart NAT applies only to ACOS devices deployed in route mode ("gateway" mode). The feature is not applicable to devices in transparent mode.
- Smart NAT uses all the multiple addresses if configured.
- Smart NAT is not supported on SIP, SIP-TCP, or SIPS virtual ports.
- VRRP-A support:
  - A floating IP addresses are required that can be reached from real servers.
  - Bind the service group to only a single virtual port. If this is not possible, ensure all virtual ports bound to the service group have the same VRID.

Example The following commands configure the VIP. Smart NAT with precedence is enabled on each virtual port.

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# source-nat auto precedence
ACOS(config-slb vserver-vport)# source-nat pool snat-pool1
ACOS(config-slb vserver)# port 21 ftp
ACOS(config-slb vserver-vport)# source-nat auto
ACOS(config-slb vserver-vport)# source-nat pool snat-pool1
```

Example The following commands configure the VIP. Smart NAT with IP-RR is enabled on each virtual port.

```
ACOS(config)# interface ve 10
ACOS(config-if:ve:10)# ip address 10.211.1.1 255.255.255.0
ACOS(config-if:ve:10)# ip allow-promiscuous-vip
ACOS(config-if:ve:10)# ipv6 address 2000::10:211:1:1/112
ACOS(config-if:ve:10)# ipv6 enable
ACOS(config-if:ve:10)# exit
ACOS(config)# interface ve 20
ACOS(config-if:ve:20)# ip address 10.212.1.1 255.255.255.0
ACOS(config-if:ve:20)# ipv6 address 2000::10:212:1:1/112
```

```
ACOS(config-if:ve:20)# ipv6 enable
ACOS(config-if:ve:20)# exit
ACOS(config)# vrrp-a vrid 1
ACOS(config-vrid:1)# floating-ip 10.212.1.222
ACOS(config-vrid:1)# floating-ip 10.212.1.223
ACOS(config-vrid:1)# floating-ip 10.212.5.1
ACOS(config-vrid:1)# floating-ip 10.212.6.1
ACOS(config-vrid:1)# floating-ip 2000::10:212:1:131
ACOS(config-vrid:1)# floating-ip 2000::10:212:1:132
ACOS(config-vrid:1)# exit
ACOS(config)# slb server rs 10.212.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server rs6 2000::10:212:1:2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group sg-tcp tcp
ACOS(config-slb svc group)# member rs 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb service-group sgv6-tcp tcp
ACOS(config-slb svc group)# member rs6 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb virtual-server vs 10.211.1.131
ACOS(config-slb vserver)# port 8081 tcp
ACOS(config-slb vserver)# service-group sg-tcp
ACOS(config-slb vserver-vport)# source-nat auto ip-rr
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
ACOS(config)# slb virtual-server vs6 2000::10:211:1:6
ACOS(config-slb vserver)# port 8080 http
ACOS(config-slb vserver)# service-group sgv6-tcp
ACOS(config-slb vserver-vport)# source-nat auto ip-rr
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

Example

The following commands shows VRRP-A support configuration examples.

Example 1: The floating IP and IP nat pool are configured using the same IP address. The IP nat pool is bound to the virtual port. In this case, the source-nat auto configuration is not supported.

```
....
ACOS(config)#ACOS(config)# ip nat pool pool1 10.212.1.222
10.212.1.222 netmask /32
ACOS(config)# vrrp-a vrid 1
ACOS(config-vrid:1)# floating-ip 10.212.1.222
....
ACOS(config)# slb virtual-server vs 10.212.1.20
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver)# service-group sg-tcp
ACOS(config-slb vserver-vport)# source-nat pool pool1
ACOS(config-slb vserver-vport)# exit
....
```

Example 2: The floating IP and source-nat auto are configured. In this case, the IP nat pool configuration is not supported. To configure source-nat auto, use a different IP address in the source-nat pool or remove the IP nat pool configuration.

```
...
ACOS(config)# interface ve 10
ACOS(config-if:ve:10)# ip address 10.211.1.1 255.255.255.0
...
ACOS(config)# vrrp-a vrid 1
ACOS(config-vrid:1)# floating-ip 10.212.1.222
....
ACOS(config)# slb virtual-server vs 10.211.1.131
ACOS(config-slb vserver)# port 8081 tcp
ACOS(config-slb vserver)# service-group sg-tcp
ACOS(config-slb vserver-vport)# source-nat auto
ACOS(config-slb vserver-vport)# exit
....
```

source-nat pool

Description Enable source NAT. Source NAT is required if the real servers are in a different subnet than the VIP.

This command is not applicable to the MMS or RTSP service types.

Syntax

```
[no] source-nat pool {pool-name | pool-group-name}
```

Parameter	Description
pool-name	Specifies the name of an IP pool of addresses to use as source addresses.
pool-group-name	Specifies the name of a group of IP address pools to use as source addresses. **NOTE:** Currently, the NAT pool-group does not support port-overload. Hence, A10 recommend to configure the NAT pool without port-overload.

Default Disabled.

Mode Virtual port

Usage This command enables source NAT using a single NAT pool or pool group, for all source addresses. If you want the ACOS device to select from among multiple pools based on source IP address, configure policy-based source NAT instead. See “access-list” on page 1.

Example The following example enables source NAT for the virtual port:

```
ACOS(config-slb vserver-vport)# source-nat pool pool2
```

source-nat use-cgnv6

Description Follow CGNv6 source NAT configuration.

Syntax

```
[no] source-nat use-cgnv6
```

Default None

Mode Virtual port

Example The following example enables source NAT for the virtual port:

```
ACOS(config-slb vserver-vport)# source-nat use-cgnv6
```

stats-data-disable

Description Disable collection of statistical data for the virtual port.

Syntax

```
stats-data-disable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual port

stats-data-enable

Description Enable collection of statistical data for the virtual port.

Syntax

```
stats-data-enable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual port

Usage To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally. (See “slb resource-usage” on page 497.)

support-http2

Description Enable HTTP/2 support.

Syntax

```
[no] support-http2
```

Default Not enabled.

Mode SLB virtual-server template

Usage This command can be configured in the following ways:

- If configured with source-nat, then ACOS will open multiple server connections for each connected client.

- If configured without source-nat, then ACOS will open only one server connection for each connected client. We support server-side HTTP/2 by mapping one-to-one relationship with the client HTTP/2 connection.

Example The following command configures HTTP/2 with source-nat.

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# source-nat pool snat-pool1
ACOS(config-slb vserver-vport)# support-http2
```

Example The following command configures HTTP/2 without source-nat.

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# support-http2
```

syn-cookie

Description Enable software-based SYN cookies for a virtual port. SYN cookies provide protection against TCP SYN flood attacks.

Syntax

```
[no] syn-cookie [expand]
```

The **expand** option enables expanded SYN cookie support. When enabled, the ACOS device can encode values for the following TCP options in the SYN-ACK:

- Windows Scale for outbound traffic (send)
- Windows Scale for inbound traffic (receive)
- Timestamp for RTTM (Round Trip Time Measurement) and PAWS (Protect Against Wrapped Sequences) mechanism.

To know detailed description of these options, refer RFC 1323 (TCP Extensions for High Performance).

Default Disabled.

Mode Virtual port

Usage For software-based SYN cookies, the ACOS device bases the maximum segment size (MSS) setting. It is the lowest MSS value supported by any

of the servers in the service group. SYN cookies on server replies to TCP health checks sent to the servers.

For hardware-based SYN cookies, refer the 'syn-cookie' global configuration command in the *Command Line Interface Reference* guide. If hardware-based SYN cookies are enabled, then software-based SYN cookies are not needed and are not used.

template

Description Apply an SLB configuration template to a virtual port.

Syntax

```
[no] template template-type template-name
```

Parameter	Description
template-type	Type of template. The template types that are available depends on the virtual port service type. To list the available template types, enter the following command: **template ?**. Some of the options are: • dns • dynamic-service • virtual-port
template-name	Name of the template.

Default If the ACOS device has a default template that is applicable to the service type, the default template is automatically applied. The ACOS device has a default virtual-port template, which is applied to a virtual port when you create it.

Mode Virtual port

Usage The normal form of this command applies the specified template to the virtual port. The **no** form of this command removes the template from the virtual port but does not delete the template itself.

A virtual port can be associated with only one template of a given type. However, the same template can be associated with more than one virtual port. To bind a virtual-port template to the port, see “template virtual-port” on page 1.

Example This following example applies to connection reuse template “reuse-template” to a virtual port:

```
ACOS(config-slb vserver-vport)# template connection-reuse
reuse-template
```

Example This following example applies to bind an existing client-ssl template to a virtual port. In this case, the TLS service is provided to the corresponding endpoint:

```
ACOS(config-slb vserver-vport)# port 53 dns
ACOS(config-slb vserver-vport)# template client_SSL
```

template virtual-port

Description Bind a virtual service port template to the virtual port.

Syntax

```
[no] template virtual-port template-name
```

Default The virtual port template of “default” is bound to virtual ports by default. Parameter settings in this default template are automatically applied to the new virtual port, until a different virtual port template is bound to the virtual port.

Mode Virtual port

Usage If a parameter is set individually on this virtual port and also is set in a virtual port template bound to this virtual port, the individual setting on this port is used instead of the setting in the template.

To configure a virtual port template, see “slb template virtual-port” on page 603.

Example These commands configure a virtual service port template named “common-vpsettings”, set the connection limit, and bind the template to a virtual port:

```
ACOS(config)# slb template virtual-port common-vpsettings
```

```
ACOS(config-vport)# conn-limit 500000
ACOS(config-vport)# exit
ACOS(config)# slb virtual-server vip1 10.10.10.99
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template virtual-port common-
vpsettings
```

template quic

Description Bind a QUIC template to the virtual server port.

Syntax

```
[no] template quic {client | server} template-name
```

Parameter	Description
template-name	Specify the name of the existing quic template.
client *template name*	Specify the name of the existing quic template that should be configured on the client side.
server *template name*	Specify the name of the existing quic template that should be configured on the server side.

Default None

Mode Virtual port

Usage Configure slb template quic and bind it to the 'quic' and 'http-over-quic' virtual ports.

The QUIC template is direction sensitive and can be configured on the client or server side.

Example The following commands bind the SLB template QUIC to the 'quic' virtual port:

```
ACOS(config)# slb virtual-server vip 10.10.10.10
ACOS(config-slb vserver)# port 443 quic
ACOS(config-slb vserver-vport)# source-nat pool p1
ACOS(config-slb vserver-vport)# template quic quic_http3
ACOS(config-slb vserver-vport)# template client-ssl ct
ACOS(config-slb vserver-vport)# template server-ssl st
```

Related Commands:

- slb template quic
- port

use-default-if-no-server

Description Forward client traffic at Layer 3, if SLB server selection fails.

Syntax

```
[no] use-default-if-no-server
```

Default Disabled. If SLB server selection fails, the traffic is dropped.

Mode Virtual port

Usage This command applies only to wildcard VIPs (VIP address 0.0.0.0).

use-rcv-hop-for-resp

Description Force the ACOS device to send replies to clients back through the last hop on which the request for the virtual port's service was received.

The 'use-rcv-hop-for-resp' option is typically used or supported in a Layer 2 (L2) networking environment.

Syntax

```
use-rcv-hop-for-resp [ src-dst-ip-swap-persist |
use-src-ip-for-dst-persist | use-dst-ip-for-src-persist ]
```

Parameter	Description
src-dst-ip-swap-persist	Creates a persistent session after the source IP and destination IP are swapped. The new persistent session should match both the source IP and the destination IP. This option should be used with the **incl-dst-ip** option for the ALG FWLB feature. This option cannot be used for the SIP protocol, because a SIP transaction may involve three or more parties.
use-src-ip-for-dst-	Creates a destination persistent session based on the source IP.

Parameter	Description
persist	
use-dst-ip-for-src-persist	Creates source-IP persistent sessions for SIP or FTP sessions by using destination IP. When enabled, the response packet go through the same firewall as the client's request packet, and the SIP session and communication sessions will be load balanced through the same firewall node.

Default Disabled.

Mode Virtual port

Usage For simple protocols, load balancing across a firewall is relatively easy. However, load balancing Application Layer Gateway (ALG) protocols, such as SIP and FTP, which have multiple connections that can originate from either side of the firewall deployment can be more challenging. The lack of predictability that occurs with ALG protocols can cause the protocol's control connection and data connection to be sent to different firewalls, thus causing the application to break.

The ACOS device uses **use-rcv-hop-for-resp** and sub-options to load balance ALG protocols through a firewall deployment consisting of paired firewalls.

For the **use-rcv-hop-for-resp** command to work for incoming packets on the default VLAN, you must also configure **vlan-global enable-def-vlan-l2-forwarding**.

Limitation The 'use-rcv-hop-for-resp' option will not work as expected for inter-partition communication. For example, if the SSLi device is setup with inside and outside partition, and the 'use-rcv-hop-for-resp' option is configured in the outside partition, this option will not work as expected. To ensure that it works correctly, configure a virtual Ethernet interface instead of an IP physical interface.

Example The following is the example of configuring **use-rcv-hop-for-resp**.

```
ACOS(config)# vlan-global enable-def-vlan-l2-forwarding
ACOS(config)# slb virtual-server outbound_wc 0.0.0.0 acl 100
```

```
ACOS(config-slb vserver)# port 0 tcp
ACOS(config-slb vserver-vport)# no-dest-nat
ACOS(config-slb vserver-vport)# service-group SG_TCP
ACOS(config-slb vserver-vport)# use-rcv-hop-for-resp
```

For more information, refer to the “ALG Protocol FWLB Support for FTP and SIP” chapter in the ***Application Delivery Controller Guide***.

To enable selecting an alternative next-hop IP address when one of the firewall or router devices fail, use the use-rcv-hop-for-resp command with 'use-rcv-hop-group' and 'server-group' options.

The following example configures **use-rcv-hop-for-resp** before the **use-rcv-hop-group** and **server-group**. These options should contain a list of valid firewall or router IP addresses.

```
ACOS(config)# slb virtual-server to-vpn
ACOS(config-slb vserver)# port 0 tcp
ACOS(config-slb vserver-vport)# use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)# use-rcv-hop-group server-group
to-vpn
ACOS(config-slb vserver-vport)# no-dest-nat
```

when-server-selection-failed

Description Configure the response to be sent to clients if server selection fails.

Syntax

```
[no] when-server-selection-failed {send-504}
```

Default Disabled

Mode SLB virtual port

Usage During HTTP load-balancing, if a configured server is not available to respond to a client's GET request, ACOS returns the HTTP 504 Gateway Timeout error.

Example The following command enables the `when-server-selection-failed` option in the HTTP port configuration:

```
ACOS(config)#slb virtual-server vs
ACOS(config-slb vserver)#port 80 http
ACOS(config-slb vserver-vport)#service-group sg-tcp
```

```
ACOS(config-slb vserver-vport)#when-server-selection-failed
send-504
```

Show Commands

show dns cache rate

Description Displays the current DNS Queries-Per-Second (QPS) and DNS cache hit rate.

Prerequisite DNS cache should be enabled either at the global configuration level or in the DNS template.

NOTE: When DNS cache is disabled, the command will display all fields as 0.

Syntax

```
show dns cache rate
```

Mode All

Usage Used to display the current DNS Queries rate (QPS) and DNS cache hit rate on-demand. It calculates the number of DNS queries received per second and those resolved from the cache per second.

Example The following example shows the response of the `show dns cache rate` command:

```
ACOS#show dns cache rate
Query rate(QPS) : 50 per second
Cache hit       : 48 per second
Cache hit ratio : 96% (cache hit/Query)
```

The following table describes the fields in the command output.

Option	Description
Query rate (QPS)	Number of DNS queries made per second.
Cache hit	Number of DNS requests per second served from the

Option	Description
	cached DNS entries.
Cache hit ratio	Calculates the ratio between the number of cache hits /number of queries made per second * 100 %.

show hardware-accelerate slb statistics

Description Displays hardware acceleration SLB statistics for the Thunder device.

Syntax `show hardware-accelerate slb statistics`

Mode All

Usage This command is only available on TH14045, TH7655 (Lite), and TH6435 devices.

Example The following command displays the hardware entries created when sessions are hardware accelerated:

```
ACOS(config)#show hardware-accelerate slb statistics
Hardware-Forwarding SLB Statistics
----------------------------------------
Current Entries                          4
Total Entries Created                    4
Total Entries Create Failure             0
Total Entries Create Failure Server Down 0
Total Entries Create Failure No More Entry 0
Total Entries Freed                      4
Total Entries Freed by Opposite Tuple Entry 2
Total Entry Free no HW Programming       0
Total Entry Free no Connection           0
Total Entry Free no SW Entry             16
Total Entries Age Out                    0
Total Entries Age Out Idle               8
Total Entries Age Out TCP FIN            8
Total Entries Age Out TCP RST            0
Total Entries Age Out Invalid DST        0
Total Entries Force HW Invalidate        0
Total Entries Invalidate Server Down     0
Current Sessions Programmed to HW        2
```

```
Total Sessions Programmed to HW                2
Total Sessions Removed from HW                 0
```

The following table describes show command output fields:

Field	Description
Current Entries	Current number of entries.
HW Entries Created	Total number of hardware entries created.
HW Entry Creation Failed	Total number of times creation of hardware entries failed.
HW Entry Creation Failed - server down	Number of times creation of hardware entries failed since the server was down.
HW Entry Creation Failed - max entries exceeded	Number of times creation of hardware entries failed since the maximum entry count exceeded.
HW Entries Freed	Total number of hardware entries freed.
HW Entries Freed - opposite tuple entry aged-out	Number of hardware entries freed since the opposite tuple entry aged-out.
HW Entry Freed - no HW prog	Number of hardware entries freed since a hardware function was unavailable.
HW Entry Freed - no matched conn	Number of hardware entries freed since no connection matched.
HW Entry Freed - no software entry	Number of hardware entries freed since the software entry was not available.
HW Entries Count	Total number of hardware entries.
HW Entries Aged Out	Total number of hardware entries that aged-out.
HW Entries Aged Out - idle timeout	Number of hardware entries that aged-out due to idle timeout.
HW Entries Aged Out - TCP FIN	Number of hardware entries that aged-out after receiving a TCP FIN packet.
HW Entries Aged Out - TCP RST	Number of hardware entries that aged-out after receiving a TCP RST packet.

Field	Description
HW Entries Aged Out - invalid dst	Number of hardware entries that aged-out due to an invalid destination address.
HW Entries Force HW Invalidate	Number of hardware entries invalidated forcefully.
HW Entries Invalidate due to server down	Number of hardware entries invalidated since the server was down.
TCAM Flows Created	Total number of TCAM flows created.
TCAM Flows Freed	Total number of TCAM flows freed.
TCAM Flow Count	Total number of TCAM flows.

show hardware-accelerate statistics

Description Displays Security Policy Engine statistics for the Thunder device when hardware acceleration is enabled.

Syntax `show hardware-accelerate statistics`

Mode All

Usage This command is only available on TH14045, TH7655 (Lite), and TH6435 devices.

Example The following command displays Security Policy Engine statistics for the Thunder device when hardware acceleration is enabled:

```
ACOS(config)# show hardware-accelerate statistics
Security Policy Engine Traffic statistics
----------------------------------------
Total Hit Counts                          5
Total IPv4 hardware Hit Counts            0
Total IPv6 hardware Hit Counts            5
Total Available IPv4 SPE Entries          131072
Total Available IPv6 SPE Entries          65536
Total IPv6 hardware forwarded packets     5
Total SPE programming requests            8
Total SPE programming errors              0
Total Ageeout Drop Counts                 0
```

```
Total Flow singlebit Errors                  0
Total Tag Mismatch Errors                    0
Total Sequence Mismatch Errors               0
Total Program Invalidation drop Counts       0
Total Flow Drop Counts                       0
Total Flow Error Counts                      0
Total Flow Unalign Counts                    0
Total Flow Underflow Counts                  0
Total Flow TX Full Drop Counts               0
Total Flow QDR Full Drop Counts              0
Total Flow Phyport Mismatch Drop Counts      0
Total Flow VLAN-ID Mismatch Drop Counts      0
Total Flow VMID Mismatch Drop Counts         0
Total Flow Protocol Mismatch Drop Counts     0
```

show hardware-accelerate status

Description Displays Security Policy Engine (SPE) status for the Thunder device.

Syntax

```
show hardware-accelerate status
```

Mode All

Usage This command is only available on TH14045, TH7655 (Lite), and TH6435 devices.

Example The following command displays SPE status:

```
ACOS(config)# show hardware-accelerate status
Security Policy Engine Status
---------------------------------------
Engine-Status                    : Initialized
Configured Profile               : ipv4-only
Engine-Setup                     : Done
Total IPv4 entries allowed       : 262144
Total IPv6 entries allowed       : 0
```

show hardware-forward slb statistics

Description Displays packet forward SLB statistics related to the Thunder 3745 and 4435 devices.

Syntax `show hardware-forward slb statistics`

Mode All

Usage This command is only available in the Thunder 3745 and 4435 devices, which are used for achieving low-latency.

Example The following example shows the counters for the Thunder device:

```
ACOS(config)#show hardware-forward slb statistics
Hardware-Forwarding SLB Statistics
----------------------------------------
Current Entries                0
Total Entries Created             0
Total Entries Create Failure          0
Total Entries Create Failure Server Down    0
Total Entries Create Failure No More Entry   0
Total Entries Freed              0
Total Entries Freed by Opposite Tuple Entry  0
Total Entry Free no HW Programming       0
Total Entry Free no Connection         0
Total Entry Free no SW Entry          0
Total Entries Age Out             0
Total Entries Age Out Idle           0
Total Entries Age Out TCP FIN         0
Total Entries Age Out TCP RST         0
Total Entries Age Out Invalid DST       0
Total Entries Force HW Invalidate       0
Total Entries Invalidate Server Down      0
Current Sessions Programmed to HW       0
Total Sessions Programmed to HW        0
Total Sessions Removed from HW         0
```

show hardware-forward statistics

Description Displays packet forward statistics related to the Thunder 3745 and 4435 devices.

Syntax `show hardware-forward statistics`

Mode All

Usage This command is only available in the Thunder 3745 and 4435 devices, which are used for achieving low-latency.

Example The following example shows the counters for the Thunder devices:

```
ACOS(config)#show hardware-forward statistics
Security Policy Engine Traffic statistics
----------------------------------------
Total Hit Counts              0
Total IPv4 hardware Hit Counts       0
Total IPv6 hardware Hit Counts       0
Total Available IPv4 SPE Entries      131072
Total Available IPv6 SPE Entries      65536
Total IPv6 hardware forwarded packets   0
Total SPE programming requests       0
Total SPE programming errors        0
Total Ageeout Drop Counts         0
Total Flow singlebit Errors        0
Total Tag Mismatch Errors         0
Total Sequence Mismatch Errors       0
Total Program Invalidation drop Counts   0
Total Flow Drop Counts           0
Total Rate Drop Counts           0
Total Flow Error Counts          0
Total Flow Unalign Counts         0
Total Flow Underflow Counts        0
Total Flow TX Full Drop Counts       0
Total Flow QDR Full Drop Counts      0
Total Flow Phyport Mismatch Drop Counts  0
Total Flow VLAN-ID Mismatch Drop Counts  0
Total Flow VMID Mismatch Drop Counts    0
Total Flow Protocol Mismatch Drop Counts  0
```

show hardware-forward status

Description Displays the status related to the Thunder 3745 and 4435 devices.

Syntax

```
show hardware-forward status
```

Mode All

Usage This command is only available in the Thunder 3745 and 4435 devices, which are used for achieving low-latency.

Example The following example shows the counters for the Thunder device:

```
ACOS(config)#show hardware-forward status
Security Policy Engine Status
-----------------------------------------
Engine-Status              : Initialized
Configured Profile         : Both ipv4-ipv6(shared)
Engine-Setup               : Done
Total IPv4 entries allowed       : 131072
Total IPv6 entries allowed       : 65536
```

show run slb template

Description Show configuration information for SLB templates. The template configuration commands in the running-config are displayed.

Syntax

```
show run slb template
[template-type
   [certificate-status]
   [default]
   [template-name]
[url-stats]
~[virtual-server]
]
[all-partitions]
[partition {shared | name}]
```

Parameter	Description
template-type	The type of SLB template configure. Enter show **slb template ?** to view a list of

Parameter	Description
	supported template types.
certificate-status	Show the status of the virtual server's certificate (OCSP-Stapling)
default	Show the configuration of the default template.
template-name	Show the configuration of the specified template.
virtual-server	Show the configuration of the specified virtual server template
all-partitions	Show SLB template configuration in all partitions.
partition	Show SLB template configuration in the specified partition only.

Mode All

Example The following command shows the template configuration commands in the running-config on an ACOS device:

```
ACOS# show run slb template
slb template udp udp-aging
   aging immediate
slb template http X-Forwarded-For
   insert-client-ip "X-Forwarded-For"
   compression minimum-content-length 120
slb template http clientip-insert
   insert-client-ip "x-Forwarded-For"
slb template http cookie-delete
   header-erase "Cookie"
slb template http hostdelete
   header-erase "Host"
slb template http hostinsert
   header-insert "Host: www.example.com"
slb template http http100
   header-insert "Expect: 100-continue"
slb template http httpinsert
   header-erase "Host"
   header-insert "Host: www.example.com"
slb template tcp-proxy tcp-timeout
  idle-timeout 180
```

```
slb template connection-reuse creuse
    timeout 60
--MORE--
```

To view the SLB virtual server template configuration

```
ACOS(config)# show run slb template virtual-server
slb template virtual-server default
  disable-when-any-port-down
!
slb template virtual-server disable-when-all
  disable-when-all-ports-down
```

To view the client SSL template URL statistics

```
ACOS(config)# show slb template client-ssl SSL-test
Category hits:
  military 0
  violence 0
  Other Categories 1

Reputation hits:
  trustworthy 2
  low-risk 1
moderate-risk 0
  suspicious 0
  malicious 0
```

show slb

Description Show statistics for SLB HTTP2.

Syntax

```
show slb http2  [detail]
```

Option	Description
detail	Lists separate counters for each CPU.

Mode All

The following table describes the fields in the command output.

Field	Description
Curr HTTP2 Sessions	Number of active HTTP2 connections that the ACOS device is servicing
Peak HTTP2 Sessions	Maximum number of HTTP2 connections the ACOS device has simultaneously serviced.
Total HTTP2 Sessions	Number of HTTP2 connections that the ACOS device has serviced
Connection Preface received	Number of HTTP2 connection prefaces received
Control Frame received	Number of HTTP2 Control frames received
Headers Frame received	Number of HTTP2 Header frames received
Continuation Frame received	Number of HTTP2 continuation frames received
RST Frame received	Number of HTTP2 RST frames received
Settings Frame received	Number of HTTP2 Settings frames received
Window Update Frame received	Number of HTTP2 Window_update frames received
Ping Frame received	Number of Ping frames received
Goaway Frame received	Number of HTTP2 Goaway frames received
Priority Frame received	Number of HTTP2 Priority frames received
Data Frame Recvd	Number of HTTP2 Data frames received
Unknown Frame Recvd	Number of frames of unknown type received
Conn preface sent	Number of HTTP2 connection prefaces sent
Setting Frame Sent	Number of HTTP2 Settings frames sent
Setting ACK Frame Sent	Number of ACK frames sent
Empty Setting Frame Sent	Number of Empty Setting frames sent

Field	Description
Ping Frame Sent	Number of Ping frames sent
Window Update Frame Sent	Number of HTTP2 Window_update frames sent
RST Frame Sent	Number of HTTP2 RST frames sent
GOAWAY Frame Sent	Number of HTTP2 Goaway frames sent
Header Frame to HTTP	Number of HTTP Header frames sent
Data Frame to HTTP	Number of HTTP Data frames sent
Protocol Error	Number of Frames received with HTTP2 Protocol_error
Internal Error	Number of Frames received with HTTP2 Internal_error
Push Promise Frame Sent	Statistics from HTTP2 Push frame count.
Unexpected PUSH_ PROMISE Frame	Statistics from HTTP2 Push Promise frame count.
Splitting Buffer Failed	Number of Buffer splitting attempt failures
Control Frame Alloc Failed	Number of control frame allocation attempt failures
Max Invalid Stream received	Maximum number of simultaneous streams flagged as invalid
Data Frame on non stream	Number of Data frames from non-dependent streams
Flow Control Error	Number of HTTP2 Flow Control frame errors
Settings Timeout	Number of settings frame sent without receiving a timely response
Frame Size Error	Number of frames received with an invalid size
Refused Stream	Number of frames received that endpoint

Field	Description
	refused prior to processing applications
Cancel	Number of frames that signify an endpoint no longer requires a data stream
Compression Error	Number of frames received with an HTTP2 compression_error
Connect Error	Number of frames received with an HTTP2 connect_error
Enhance Your Calm Error	Number of frames received with an HTTP2 enhance_your_calm error
Inadequate Security	Number of frames received with an inadequate_security code
HTTP1.1 Required	Number of frames received with an HTTP_ 1_1 required code
Deflate Alloc Fail	Number of deflation allocation failures
Inflate Alloc Fail	Number of inflation allocation failures
Inflate Header Fail	Number of headers with inflation failures
Bad Connection Preface	Number of bad connection preface frame errors
Cannot Alloc Control Frame	Number of control frames for which resources could be be allocated
Cannot Alloc Settings Frame	Number of setting frames for which resources could be be allocated
Bad Frame Type for Stream	Number of bad frames
Wrong Stream State	Number of frames with wrong frame
Data Queue Alloc Error	Number of data frames from which resources could be be allocated
Buff Alloc Error	Number of buffers for which resources could be be allocated
Cannot Alloc Rst Frame	Number of RST frames for which resources

Field	Description
	could be be allocated
Cannot Alloc Goaway Frame	Number of goaway frames for which resources could be be allocated
Cannot Alloc Ping Frame	Number of ping frames for which resources could be be allocated
Cannot Alloc Stream	Number of stream frames for which resources could be be allocated
Cannot Alloc Window Frame	Number of window frames for which resources could be be allocated
Header No Stream	Number of headers for which no stream was processed
Header Padlen Too Large	Number of data frames with excessive padding bytes
Too Many Streams	Number of times the maximum number of streams was exceeded
Unexpected Frame in Idle	Number of times idle frame was in unexpected place within a stream
Unexpected Frame in Rsvd Local	Number of times Reserved Local frame was in unexpected place within a stream
Unexpected Frame in Rsvd Remote	Number of times Reserved Remote frame was in unexpected place within a stream
Unexpected Frame in Half Close Remote	Number of times Half Close Remote frame was in unexpected place within a stream
Unexpected Frame in Closed	Number of times Closed frame was in unexpected place within a stream
Window Update with 0 Increment	Number of Window Update frames with no increment
Window Update Increment Too Large	Number of Window Update frames with excessive increment
Stream Closed	Number of streams that the device has closed

Field	Description
Continuation Frame with No Headers	Number of continuation streams received with no corresponding header frame
Unexpected Frame Before Headers Complete	Number of streams with data frames before the header completes
Headers Frame Before Cont Complete	Number of streams with header frames before continuation completes
Unexpected Push Promise Frame	Number of unexpect push of representation from servers to client
Received Invalid Stream ID	Number of frames received with invalid stream ID
Headers Interleaved on Streams	Maximum number of headers that are interleaved within the HTTP2 stream
Trailer Frame Not Marked End of Stream	Number of streams not terminated with an End of Stream frame
Invalid Setting Value	Number of frames with invalid setting value
Invalid Window-Update Value	Number of frames with invalid window-update values
Frame Header Bytes received	Number of HTTP2 frame header bytes the ACOS device received
Frame Header Bytes Sent	Number of HTTP2 frame header bytes the ACOS device sent
Control Frame Bytes received	Number of HTTP2 control frame bytes the ACOS device received
Control Frame Bytes Sent	Number of HTTP2 control frame bytes the ACOS device sent
Header Bytes received	Number of HTTP2 header bytes the ACOS device received
Header Bytes Sent	Number of HTTP2 header bytes the ACOS device sent

Field	Description
Data Bytes received	Number of HTTP2 data bytes the ACOS device received
Data Bytes Sent	Number of HTTP2 data bytes the ACOS device sent
Total Bytes received	Number of HTTP2 bytes the ACOS device received
Total Bytes Sent	Number of HTTP2 bytes the ACOS device sent

Example The following command shows HTTP2 statistics:

```
ACOS# show slb http2 | section HTTP2
Curr HTTP2 Session                  0
Peak HTTP2 Session                  0
Total HTTP2 Session                 0

ACOS# show slb http2 detail
                                    DP0         DP1
Total
-------------------------------------------------------------------
----
Curr HTTP2 Sessions                 0           0           0
Peak HTTP2 Sessions                 0           0           0
Total HTTP2 Sessions                0           0           0
Connection Preface received         0           0           0
Control Frame received              0           0           0
Headers Frame received              0           0           0
Continuation Frame received         0           0           0
RST Frame received                  0           0           0
Settings Frame received             0           0           0
Window Update Frame received        0           0           0
Ping Frame received                 0           0           0
Goaway Frame received               0           0           0
Priority Frame received             0           0           0
Data Frame Recvd                    0           0           0
Unknown Frame Recvd                 0           0           0
Conn preface sent                   0           0           0
Setting Frame Sent                  0           0           0
```

Setting ACK Frame Sent	0	0	0
Empty Setting Frame Sent	0	0	0
Ping Frame Sent	0	0	0
Window Update Frame Sent	0	0	0
RST Frame Sent	0	0	0
GOAWAY Frame Sent	0	0	0
Header Frame to HTTP	0	0	0
Data Frame to HTTP	0	0	0
Protocol Error	0	0	0
Internal Error	0	0	0
HTTP2 Proxy alloc Error	0	0	0
Push Promise Frame Sent	11		
Unexpected PUSH_PROMISE Frame	1		
Splitting Buffer Failed	0	0	0
Control Frame Alloc Failed	0	0	0
Max Invalid Stream received	0	0	0
Data Frame on non stream	0	0	0
Flow Control Error	0	0	0
Settings Timeout	0	0	0
Frame Size Error	0	0	0
Refused Stream	0	0	0
Cancel	0	0	0
Compression Error	0	0	0
Connect Error	0	0	0
Enhance Your Calm Error	0	0	0
Inadequate Security	0	0	0
HTTP1.1 Required	0	0	0
Deflate Alloc Fail	0	0	0
Inflate Alloc Fail	0	0	0
Inflate Header Fail	0	0	0
Bad Connection Preface	0	0	0
Cannot Alloc Control Frame	0	0	0
Cannot Alloc Settings Frame	0	0	0
Bad Frame Type for Stream	0	0	0
Wrong Stream State	0	0	0
Data Queue Alloc Error	0	0	0
Buff Alloc Error	0	0	0
Cannot Alloc Rst Frame	0	0	0
Cannot Alloc Goaway Frame	0	0	0
Cannot Alloc Ping Frame	0	0	0

```
Cannot Alloc Stream                    0          0          0
Cannot Alloc Window Frame              0          0          0
Header No Stream                       0          0          0
Header Padlen Too Large                0          0          0
Too Many Streams                       0          0          0
Unexpected Frame in Idle               0          0          0
Unexpected Frame in Rsvd Local         0          0          0
Unexpected Frame in Rsvd Remote        0          0          0
Unexpected Frame in Half Close Remote  0          0          0
Unexpected Frame in Closed             0          0          0
Window Update with 0 Increment         0          0          0
Window Update Increment Too Large      0          0          0
Stream Closed                          0          0          0
Continuation Frame with No Headers     0          0          0
Unexpected Frame Before Headers Complete 0        0          0
Headers Frame Before Cont Complete     0          0          0
Unexpected Push Promise Frame          0          0          0
Received Invalid Stream ID             0          0          0
Headers Interleaved on Streams         0          0          0
Trailer Frame Not Marked End of Stream 0          0          0
Invalid Setting Value                  0          0          0
Invalid Window-Update Value            0          0          0
Frame Header Bytes received            0          0          0
Frame Header Bytes Sent                0          0          0
Control Frame Bytes received           0          0          0
Control Frame Bytes Sent               0          0          0
Header Bytes received                  0          0          0
Header Bytes Sent                      0          0          0
Data Bytes received                    0          0          0
Data Bytes Sent                        0          0          0
Total Bytes received                   0          0          0
Total Bytes Sent                       0          0          0
```

show slb aflow

Description Show aFlow statistics.

Syntax

```
show slb aflow [detail]
```

Parameter	Description
`detail`	List separate counters for each CPU in the statistics output.

Mode All

The following table describes the fields in the command output.

Field	Description
Pause connection	Number of pause connection in the aFlow queue. The aFlow maximum queue limit is 65,535.
Pause connection fail	Number of failed connections added in the aFlow paused queue after reaching the maximum limit.
Resume connection	Number of resumed connections from the aFlow paused queue. It gets incremented when the connection is deleted from the aFlow paused queue.
Open new server conn	Number of connections that are opened in a new server from the aFlow. It gets incremented when the existing connection is closed and there are no more existing connection that can be re-used when aFlow resumes the connection from the paused queue.
Reuse idle server conn	It gets incremented when the aFlow paused queue reaches its limit, and needs to reuse the idle connection, which is already in the server.

Example The following command shows aFlow statistics:

```
ACOS# show slb aflow
               Total
-------------------------------------------
Pause connection                   80564
Pause connection fail                  0
Resume connection                  61804
Open new server conn                  13
Reuse idle server conn                 0
```

show slb attack-prevention

Description Show SYN-cookie statistics for the number of packets received during different intervals of time.

Syntax

```
show slb attack-prevention
```

Mode All

Usage When running the **show slb attack-prevention** command on an FTA-enabled model, the “SYN attack” field does not show output for the historical counters (1s/5s/30s/1min/5min). Output is only provided for the “current” column.

This feature is supported for L3V private partitions in non-FTA-enabled models. If the **show slb attack-prevention** command is run from an L3V partition on an FTA-enabled model, the “SYN attack” counter displays zero for all columns.

Example The following command shows SYN-cookie statistics:

```
ACOS# show slb attack-prevention
                         Current    1 sec  5 sec  30 sec  1
min  5 min
-------------------------------------------------------------
-----------
SYN cookie snt           0          0      0       0       0
  0
SYN cookie snt ts        0          0      0       0       0
  0
```

```
SYN cookie snt fail       0           0       0       0       0
  0
SYN cookie chk fail       0           0       0       0       0
  0
SYN attack                0           0       0       0       0
  0
```

The following table describes the fields in the command output.

Field	Description
SYN cookie snt	Number of TCP SYN cookies sent.
SYN cookie snt ts	Number of expanded TCP SYN cookies sent.
SYN cookie snt fail	Number of TCP SYN cookie send attempts that failed.
SYN cookie chk fail	Number of TCP SYN cookies for which the responding ACK failed the SYN cookie check.
SYN attack	Total number of SYN connections that did not receive an ACK from the client and assumed to be SYN attack.

show slb cache

Description Display statistics and other information for RAM caching.

Syntax

```
show slb cache
[entries vip-name port-num [url | detail] |
memory-usage |
replacement vip-name port-num |
stats [vip-name port-num]]
```

Option	Description
entries *vip-name*	Shows a list of the cached objects for the specified VIP and virtual port.

Option	Description
port-num	You can specify a *url* to further refine the statistics shown for each cached entry/URL maintained under a cache template that is bound to a virtual port. • If certain headers are present in the server response, such as Age, Via, Connection, they will be removed and the ACOS device will add a separate header for them before the response is stored in cache. Similarly if the cache template has the remove-cookies option set, any cookie header in the server response will be removed before saving the same in cache. • If the *url* includes special characters such as a question mark, the character must be represented in its octal notation as (for example, \077 for the question mark) in the URL string. A URL name such as "/testing?html" is specified as "/testing\077html" and it must be enclosed within double quotes to ensure that it is interpreted correctly.
memory-usage	Shows memory usage for RAM caching.
replacement *vip-name port-num*	Shows replacement information for the specified virtual port on the specified virtual server.
stats [*vip-name port-num*]	Lists RAM caching statistics by VIP. If you specify a VIP or port number, statistics are displayed only for that VIP or port number.

Mode All

Usage If you do not use any of the optional parameters, RAM caching statistics are displayed. This is equivalent to entering the **show slb cache stats** command.

Example The following command shows RAM caching statistics:

```
ACOS# show slb cache
Total
-----------------------------------------------------------------
-
Cache Hits                0          (0.0 %)
Cache Misses              0
Memory Used               0
Bytes Served              0

Requests
  - Total Requests        0
  - Cacheable Requests    0
  - No-cache Requests     0
  - IMS Requests          0

Responses (from server)
  - 304 Not Modified      0
  - 200 OK - Cont Len     0
  - 200 OK - Chnk Enc     0
  - 200 OK - Other        0
  - Not cacheable         0

Responses (from cache)
  - 304 Not Modified      0
  - 200 OK - No Comp      0
  - 200 OK - Gzip         0
  - 200 OK - Deflate      0
  - Other                 0

Entries
  - Cached                0
  - Replaced              0
  - Aged Out              0
  - Cleaned               0
  - Create failures       0

Revalidation
  - Successes             0
  - Failures              0
```

```
Policies
  - URI nocache           0
  - URI cache             0
  - URI invalidate        0
  - Content Too Big       0
  - Content Too Small     0
```

The following table describes the fields in the command output.

Field	Description
Cache Hits	Number of times a requested page was found in the cache and served from the cache.
Cache Misses	Number of times a requested page was not found in the cache.
Memory Used	Amount of RAM currently used by cached content.
Bytes Served	Number of bytes served.
Requests	Contains the following conters: • Total Requests – Total number of requests received on all virtual server ports on which caching is configured. • Cacheable Requests – Number of requests that are potentially cacheable. • No-cache Requests – Number of requests with no-cache header directives. • IMS Requests – Number of requests that contained an If-Modified-Since header.
Responses (from server)	Contains the following counters: • 304 Not Modified – Number of “304 Not Modified” responses sent from the server. • 200 OK - Cont Len – Number of “200 OK - Cont Len” responses sent to clients. • 200 OK - Chnk Enc – Number of “200 OK - Chnk

Field	Description
	Enc" responses sent to clients. • 200 OK - Other – Number of "200 OK - Other" responses sent to clients. • Not cacheable – Number of responses with no-cache header directives.
Responses (from cache)	Contains the following counters: • 304 Not Modified – Number of "304 Not Modified" responses sent from the cache. • 200 OK - No Comp – Number of "200 OK - No Comp" responses sent from the cache. "No Comp" indicates that the object is not compressed. • 200 OK - Gzip – Number of "200 OK - Gzip" responses sent from the cache. This indicates that an object was compressed using gzip. Gzip is an encoding format produced by the file compression program "gzip" (GNU zip) as described in RFC 1952 (Lempel-Ziv coding [LZ77] with a 32 bit CRC). • 200 OK - Deflate – Number of "304 Not Modified" responses sent from the cache. This indicates that an object was compressed using deflate. Deflate is the "zlib" format defined in RFC 1950 in combination with the "deflate" compression mechanism described in RFC 1951. • Other – Number of "Other" responses sent from the cache. This indicates that an object was compressed using compress. Compress is the encoding format produced by the common UNIX file compression program "compress" (adaptive Lempel-Ziv-Welch coding [LZW]).
Entries	Contains the following counters: • Cached – Number of objects currently in the

Field	Description
	cache. • Replaced – Number of cached items that were removed to make room for newer entries, per the replacement policy. • Aged Out – Number of entries that were removed because they are older than their expiration time. • Cleaned – Number of cached objects that have aged out and therefore been removed from the cache. • Create Failures – Number of times ACOS failed to create a cache entry.
Revalidation	Contains the following counters: • Successes – Number of entries that were successfully revalidated by the server. • Failures– Number of times revalidation failed.
Policies	Contains the following counters: • URI nocache – Number of times requested content was not cached due to a URI policy. • URI cache – Number of times a request was cached due to a URI policy. • URI invalidate – Number of times a request was invalidated due to a URI policy. • Content Too Big – Number of cacheable items that were not cached because the file size was larger than the configured maximum content size. • Content Too Small – Number of cacheable items that were not cached because the file size was smaller than the configured minimum content size.

Example The following command shows cached objects:

```
ACOS# show slb cache entries vs-cookie-cache 80
vs-cookie-cache:80
Host            Object URL            Bytes    Type  Status
Expires in
-----------------------------------------------------------------
-------
10.20.0.120     /static2/1000.txt     1365     CL,No   FR
   3410 s
10.20.0.120     /static2/10000.txt
   10366   CL,No   FR    3490 s
10.20.0.120     /static2/1000000.txt  636152
 CE,Gz   FR    3594 s
10.20.0.120     /static2/1000000.txt  1000368 CL,No   FR
 2719 s
10.20.0.120     /ewen/index.html      1479     CL,Mo   FR    -
57 s
```

The following table describes the fields in the command output.

Field	Description
cached-vip	Virtual port number on which RAM caching is enabled.
Host	IP address of the content server.
Object URL	URL from which the cached object was obtained by the ACOS device.
Bytes	Length of the cached object.
Type	Indicates whether the cached object has a Content-Length header, is compressed, or is chunk-encoded. The value after the comma indicates the type of compression used: • No – Object is uncompressed. • Gz – Object was compressed using gzip. Gzip is an encoding format produced by the file compression program “gzip” (GNU zip) as described in RFC 1952 (Lempel-Ziv coding [LZ77] with a 32 bit CRC).

Field	Description
	• Cm – Object was compressed using compress. Compress is the encoding format produced by the common UNIX file compression program “compress” (adaptive Lempel-Ziv-Welch coding [LZW]). • Df – Object was compressed using deflate. Deflate is the “zlib” format defined in RFC 1950 in combination with the “deflate” compression mechanism described in RFC 1951.
Status	Status of the entry: • FR – Fresh • ST – Stale • IN – Incomplete • FA – Failed • UN – Unknown • R – The entry must be revalidated.
Expires in	Number of seconds the object can remain unused before it ages out.

Example

The following command shows RAM caching memory usage:

```
ACOS# show slb cache memory-usage
VIP             Port   Memory Configured  Memory Used
Percent Used
-------------------------------------------------------------
-------
vs120            80     10485760           8386560
79.98%
-------------------------------------------------------------
-------
Total                   10485760           8386560
79.98%
```

NOTE: The "Memory Used" value checked with this command may differ from the actual memory consumption. To check the actual memory consumption, you need to verify the increments using "show memory".

Example The following command shows replacement statistics:

```
ACOS# show slb cache replacement cached-vip 80
Frequency                  Total
-------------------------------------------------------------
-
1/256                      6
1/128                      0
1/64                       0
1/32                       0
1/16                       0
1/8                        0
1/4                        0
1/2                        0
1                          0
2                          0
4                          0
8                          0
16                         0
32                         0
64                         0
128                        2
```

The output shows the distribution of requests for the cached entries. Entries listed for 1/256 (one in 256 requests) are the least requested, whereas entries listed for 128 are the most requested.

show slb common

Description Show common SLB information.

Syntax

```
show slb common
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb common
Server auto Reselect: 1
```

Field	Description
Server auto Reselect	Indicates whether server auto-reselection is enabled or disabled .

show slb compression

Description Show HTTP compression statistics in bytes.

Syntax

```
show slb compression
[virtual-server port-num]
[all-partitions | partition {shared | name}]
```

Option	Description
virtual-server port-num	Show HTTP compression statistics for the specified virtual server only. The *port-num* option shows information only for the specified virtual port on the virtual server.
all-partitions	Show HTTP compression statistics in all partitions.
partition {**shared** | *name*}	Show HTTP compression statistics in the specified partition or shared partition.

Mode All

show slb connection-reuse

Description Show SLB connection-reuse statistics.

Syntax

```
show slb connection-reuse [detail]
```

Parameter	Description
detail	List separate counters for each CPU in the statistics output.

Mode All

Example The following command shows summary connection-reuse statistics:

```
ACOS# show slb connection-reuse
                          Total
-------------------------------------------------------------------
----
Open persist              0
Active persist            0
Total established         1787
Total terminated          1787
Total terminated by err   0
Total bind                1277
Total unbind              2389
Delayed unbind            4
Long resp                 0
Missed resp               0
Unbound data received     0
Pause request             0
Pause request fail        0
Resume request            0
Not remove from list      0
```

The following table describes the fields in the command output.

Field	Description
Open persist	Number of new client connections directed to the same server as previous connections by the persistence feature.
Active persist	Number of currently active connections that were sent to the same real server by the persistence feature.

Field	Description
Total established	Total number of established connections to the backend server.
Total terminated	Total number of terminated connections to the backend server.
Total terminated by err	Total Number of backend connections terminated due to an error.
Total bind	Total number of client persistent connections bound to the backend server.
Total unbind	Total number of client persistent connections unbound from the backend server.
Delayed unbind	Number of connections whose unbinding was delayed. **NOTE:** In the current release, this counter is unused and is always 0.
Long resp	Number of responses that took too long.
Missed resp	Number of missed responses to HTTP requests.
Unbound data received	Amount of data received on an unbound connection. This is used for debugging purposes.
Pause request	These are internal counters used by A10 Technical Support for debugging purposes.
Pause request fail	
Resume request	
Not remove from list	

show slb conn-rate-limit

Description Show statistics for source-IP based connection rate limiting.

Syntax

```
show slb conn-rate-limit src-ip
{locked-out-ips | statistics [debug]}
```

Mode All

Example This command shows statistics for source-IP based connection rate limiting:

```
ACOS(config)# show slb conn-rate-limit src-ip statistics
Sessions allocated 0
Sessions freed 0
Too many sessions consumed 0
Out of sessions 0
Threshold check count 1022000
Honor threshold count 20532
Threshold exceeded count 1001408
Lockout drops 60
Log messages sent 20532
DNS requests re-transmitted  1000
No DNS response for request 1021000
```

The following table describes the fields in the show command output.

Field	Description
Sessions allocated	Number of sessions allocated.
Sessions freed	Number of sessions freed.
Too many sessions consumed	Number of times too many sessions were consumed.
Out of sessions	Number of times the device ran out of sessions.
Threshold check count	Number of times the ACOS device has checked for connection-limit violations.
Honor threshold count	Number of requests permitted because they were within the connection limit.

Field	Description
Threshold exceeded count	Number of requests denied because they exceeded the connection limit.
Lockout drops	Number of requests dropped because a client was locked out.
Log messages sent	Number of log messages generated by this feature.
DNS requests re-transmitted	Number of re-transmitted DNS requests detected. These are DNS requests for which no response was received by the ACOS device.
No DNS response for request	Number of DNS requests for which no response was received.

show slb ddos-protection l4-entries

Description This command displays abnormal L4 port entries from DDoS monitoring and selective filtering.

Syntax

```
show slb ddos-protection l4-entries
[address ipaddr | in-hardware | l4-proto protocol-num |
not-in-hardware | port port-num]
```

Example The following example displays sample output:

```
ACOS(config)# show slb ddos-protection l4-entries
Address          L4    Port    PPS
-----------------------------------
1.1.1.1          17    333     5000
```

Usage The following table describes the fields for the show command output:

Field	Description
Address	The destination IP address that traffic is matched to.
L4	The Layer 4 protocol type. In the above example, L4 17

Field	Description
	indicates UDP traffic.
Port	The specific destination IP port that traffic is matched to.
HW?	This indicates whether or not the entry is programmed into the hardware. A “Y” means the entry is programmed into the hardware, and an “N’” means it is not.
Pkts in last 10 sec	The number of packets that match the IP address and the given port in the last 10 seconds.

show slb ddos-protection statistics

Description This command displays the logging statistics for SLB DDoS selective filtering.

Syntax

```
show slb ddos-protection statistics
```

Mode All

Example The following is a sample output:

```
ACOS# show slb ddos-protection statistics
L3 Entry Added                          0
L3 Entry Deleted                        0
L3 Entry Added to BGP                   0
L3 Entry Removed From BGP               0
L3 Entry Added to HW                    0
L3 Entry Removed From HW                0
Too Many L3 entries                     0
L3 Entry Match Drop                     0
HW L3 Entry Match Drop                  0
L4 Entry Added                          3
L4 Entry Deleted                        2
L4 Entry Added to HW                    3
L4 Entry Removed From HW                1
HW out of L4 Entries                    0
L4 Entry Match Drop                     5
HW L4 Entry Match Drop                  2153756264
```

show slb dns-custom-logging-keywords

Description Shows the available predefined keywords that can be used in custom log formats within the DNS logging template.

Syntax

```
show slb dns-custom-logging-keywords [request | response | timeout]
```

Parameter	Description
request	Show available keywords for custom DNS request log messages.
response	Show available keywords for custom DNS response log messages.
timeout	Show available keywords for custom DNS timeout log messages.

Mode All

Description The custom log format allows you to include supported DNS logging fields within the DNS logging template by using predefined keywords. These keywords can be used to construct meaningful and detailed log entries for request, response, and timeout events. For more information, see *DNS Logging* chapter in the *Application Delivery Controller Guide.*

Example The following table lists all the supported custom logging keywords, trigger reasons, and example values:

Keyword	Description	Example Output in logs	response	request	timeout
$queryid$	Query ID used in the DNS logging.	2BD8	√	√	√
$opcode$	Opcode used in the DNS	0-F	√	√	√

Keyword	Description	Example Output in logs	response	request	timeout
	logging.				
$headerflag$	Header flag used in the DNS logging.	RD|RA	√	√	√
$recordcounters$	Combination of qdcount, ancount, nscount, arcount used.	1|1|0|0	√	√	√
$qdcount$	Number of questions (QDCOUNT) used in the DNS logging.	1	√	√	√
$ancount$	Number of answers (ANCOUNT) used in the DNS logging.	1	√	√	√
$nscount$	Number	0	√	√	√

Keyword	Description	Example Output in logs	response	request	timeout
	of authority records (NSCOUNT) used in the DNS logging.				
$arcount$	Number of additional records (ARCOUNT) used in the DNS logging.	0	√	√	√
$respsrc$	Response source information used.	gslb/cache/backend/rpz	√	X	X
$queryname$	DNS query name used.	dns.example.com	√	√	√
$querytype$	DNS query type used.	A	√	√	√

Keyword	Description	Example Output in logs	response	request	timeout
`$queryclass$`	DNS query class used.	IN	√	√	√
`$queryinfo$`	Combination of information with query name, query type, query class used.	dns.example.com A IN	√	√	√
`$rcode$`	DNS response (rcode) used.	0000-FFFF	√	√	X
`$rcodestr$`	DNS response code (string format).	0 NoError No Error [RFC 1035] 1 FormErr Format Error [RFC 1035] 2 ServFail Server Failure [RFC 1035] 3 NXDomain Non-Existent Domain [RFC 1035] 4 NotImp Not Implemented	√	√	X

Keyword	Description	Example Output in logs	response	request	timeout
		[RFC 1035] 5 Refused Query Refused [RFC 1035] 6 YXDomain Name Exists when it should not [RFC 2136] 7 YXRRSet RR Set Exists when it should not [RFC 2136] 8 NXRRSet RR Set that should exist does not [RFC 2136] 9 NotAuth Server Not Authoritative for zone [RFC 2136] 10 NotZone Name not contained in zone [RFC 2136]			
`$respsec$`	Combination of all response records like answer, authority and additional	Answer section [record1;record2; record3] Authority section [record1;record2; record3] Addition section [record1;record2; record3]	√	X	X

Keyword	Description	Example Output in logs	response	request	timeout
	records.				
$anssec$	Answer section records used.	Answer section [record1;record 2; record3]	√	X	X
$authsec$	Authority section records used.	Authority section [record1;record 2; record3]	√	X	X
$addsec$	Additional section records used.	Addition section [record1;record 2; record3]	√	X	X
src	Packet source IP address used in the DNS logging.	20.20.20.20	√	√	√
dst	Packet destination IP address used in the DNS logging.	20.20.40.4	√	√	√
spt	Packet source port	10012	√	√	√

Keyword	Description	Example Output in logs	response	request	timeout
	used in the DNS logging.				
`$dpt$`	Packet destination port used in the DNS logging.	53	√	√	√
`$proto$`	Packet protocol used in the DNS logging.	UDP	√	√	√
`$snatinfo$`	Source NAT information.	20.20.40.1#43014	√	X	√

Example The following example shows the request-specific keywords:

```
ACOS# show slb dns-custom-logging-keywords request
$queryid$       query id
$opcode$       opcode
$headerflag$    headerflag
$recordcounters$  record counters
$qdcount$       qdcount
$ancount$       ancount
$nscount$       nscount
$arcount$       arcount
$queryname$      query fqdn
$querytype$      dns type
$queryclass$    dns class
$queryinfo$      query information
$rcode$        dns rcode
$rcodestr$      dns rcode string
$src$         packet source ip
$dst$         packet destination ip
$spt$         packet source port
$dpt$         packet destination port
$proto$        packet protocol
```

Example The following example shows the response-specific keywords:

```
ACOS# show slb dns-custom-logging-keywords response
$queryid$       query id
$opcode$       opcode
$headerflag$    headerflag
$recordcounters$  record counters
$qdcount$       qdcount
$ancount$       ancount
$nscount$       nscount
$arcount$       arcount
$respsrc$       response source
$queryname$     query fqdn
$querytype$     dns type
$queryclass$    dns class
$queryinfo$     query information
$rcode$        dns rcode
$rcodestr$     dns rcode string
$respsec$       all response records
$anssec$       answer records
$authsec$       auth records
$addsec$       additional records
$src$         packet source ip
$dst$         packet destination ip
$spt$         packet source port
$dpt$         packet destination port
$proto$        packet protocol
$snatinfo$     NAT info
```

Example The following example shows the timeout-specific keywords:

```
ACOS# show slb dns-custom-logging-keywords timeout
$queryid$       query id
$opcode$       opcode
$headerflag$    headerflag
$recordcounters$  record counters
$qdcount$       qdcount
$ancount$       ancount
$nscount$       nscount
$arcount$       arcount
$queryname$      query fqdn
$querytype$      dns type
$queryclass$    dns class
$queryinfo$      query information
$src$         packet source ip
$dst$         packet destination ip
$spt$         packet source port
$dpt$         packet destination port
$proto$        packet protocol
$snatinfo$      NAT info
```

show slb diameter

Description Show statistics for Diameter load balancing.

Syntax

```
show slb diameter [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.
device *DeviceID*	If the ACOS device is a member of an aVCS, use this option to specify the device ID to which this command must apply. If you omit this option, the command is applied to the vMaster. However, if you have changed the device context of the management session from the vMaster to another device, and you omit the **device** option, the command is applied only to the other device (the one to which you set the device context).

Mode All

Example The following command shows statistics for Diameter load balancing:

```
ACOS# show slb diameter
                            Total
-------------------------------------------------------------
----
concurrent user-session   0
acr out                   0
acr in                    0
aca out                   0
aca in                    0
dpr out                   0
dpr in                    0
dpa out                   0
dpa in                    0
cea out                   0
cea in                    0
cer out                   0
cer in                    0
dwa out                   0
dwa in                    0
dwr out                   0
dwr in                    0
str out                   0
str in                    0
sta out                   0
sta in                    0
asr out                   0
asr in                    0
asa out                   0
asa in                    0
other out                 0
other in                  0
mismatch fwd session id   0
mismatch rev session id   0
unknown command code      0
no session id drop        0
no fwd tuple drop         0
no rev tuple drop         0
```

```
cross cpu fwd send          0
cross cpu fwd rcv           0
cross cpu rev send          0
cross cpu rev rcv           0
cross cpu fail              0
retry client req            0
retry client req fail       0
reply unknown session id    0
ccr out                     0
ccr in                      0
cca out                     0
cca in                      0
ccr initial                 0
ccr update                  0
ccr termination             0
cca termination             0
term session on cca-t       0
fwd unknown session id      0
update latest server        0
client selection failure    0
close conn by virtual portdown  0
invalid avp                 0
reselect fwd tuple          0
reselect fwd tuple cross    0
reselect rev tuple          0
conn closed by client       0
conn closed by server       0
reply invalid avp value     0
reply unable to deliver     0
reply error info fail       0
ACOS#
```

The following table describes the fields in the command output.

Field	Description
concurrent user-session	Number of concurrent user sessions.
acr out	Number of Accounting-Request messages sent by the ACOS device.

Field	Description
acr in	Number of Accounting-Request messages received by the ACOS device.
aca out	Number of Accounting-Answer messages sent by the ACOS device.
aca in	Number of Accounting-Answer messages received by the ACOS device.
cea out	Number of Capabilities-Exchange-Answer messages sent by the ACOS device.
cea in	Number of Capabilities-Exchange-Answer messages received by the ACOS device.
cer out	Number of Capabilities-Exchange-Request messages sent by the ACOS device.
cer in	Number of Capabilities-Exchange-Request messages received by the ACOS device.
dwr out	Number of Device-Watchdog-Request messages sent by the ACOS device.
dwr in	Number of Device-Watchdog-Request messages received by the ACOS device.
dwa out	Number of Device-Watchdog-Answer messages sent by the ACOS device.
dwa in	Number of Device-Watchdog-Answer messages received by the ACOS device.
str out	Number of Session-Termination-Request messages sent by the ACOS device.
str in	Number of Session-Termination-Request messages received by the ACOS device.
sta out	Number of Session-Termination-Answer messages sent by the ACOS device.
sta in	Number of Session-Termination-Answer messages received by the ACOS device.
asr out	Number of Abort-Session-Request messages sent by

Field	Description
	the ACOS device.
asr in	Number of Abort-Session-Request messages received by the ACOS device.
asa out	Number of Abort-Session-Answer messages sent by the ACOS device.
asa in	Number of Abort-Session-Answer messages received by the ACOS device.
other out	Number of other types of Diameter messages (other codes) sent by the ACOS device.
other in	Number of Diameter messages of other types received by the ACOS device.
ccr out	Total Credit-Control-Request messages sent.
ccr in	Total Credit-Control-Request messages received.
cca out	Total Credit-Control-Answer messages sent.
cca in	Total Credit-Control-Answer messages received.
ccr initial	Total Credit-Control-Request-initial messages received.
ccr update	Total Credit-Control-Request-update messages received.
ccr termination	Total Credit-Control-Request-termination messages received.
cca termination	Total Credit-Control-Answer-termination messages received.
term session on cca-t	Total sessions ACOS terminated for Credit-Control-Answer-Termination.
mismatch fwd session id	Client session ID does not match Diameter session table.
mismatch rev session	Server session ID does not match Diameter session table.

Field	Description
id	
unknown command code	Drop Diameter session because of unrecognized command code.
no session id drop	Cannot find session ID AVP in the message, drop request.
no fwd tuple drop	Cannot match client L4 session, drop message.
no rev tuple drop	Cannot match server L4 session, drop message.
cross cpu fwd send	Number of client messages sent to server using different CPU.
cross cpu fwd rcv	Number of client messages received by different CPU and sent to server.
cross cpu rev send	Number of server message sent to client using different CPU.
cross cpu rev rcv	Number of server message received by different CPU and sent to client.
cross cpu fail	Number of failures during cross CPU process.
retry client req	Number of times reselect is performed and a different server is chosen.
retry client req fail	Failure counter for retry client features.
reply unknown session id	Total unknown-session-id messages sent with error-code 5002.
invalid avp	Attribute Value Pair (avp) value contains illegal characters.
reselect fwd tuple	Original client tuple does not exist, so reselect another one on the same CPU.
reselect fwd	Original client tuple does not exist, so reselect

Field	Description
tuple cross	another one on another CPU because there is none on the current CPU.
reselect rev tuple	Original server tuple does not exist, so reselect another one. There should always be a server side connection on the current CPU so there is no counter for “reselect rev tuple cross”.
conn closed by client	Client side connection was terminated by client (client initiated fin/reset).
conn closed by server	Server side connection was terminated by server (server initiated fin/reset).
reply invalid avp value	Reply to sender (client or server) with error info “invalid avp value” when incoming message has invalid avp value.
reply unable to deliver	Reply to sender (client or server) with error info “unable to deliver” when an incoming message cannot be forwarded.
reply error info fail	Fail to reply to client or server with error info.

show slb fast-fix

Description Displays the statistics and performance metrics for the Fast FIX.

Syntax

```
show slb fast-fix
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb fast-fix
```

```
                                        Total
-----------------------------------------------
Insert client IP                          0
Default switching                         0
Sender ID switching                       0
Target ID switching                       0
```

Field	Description
Insert client IP	Number of times the client IP was inserted in the header.
Default switching	Number of times default switching occurred.
Sender ID switching	Number of times switching occurred based on the sender's ID.
Target ID switching	Number of times switching occurred based on the target's ID.

show slb fast-http-proxy

Description Show statistics for SLB fast-HTTP proxy.

Syntax **show slb fast-http-proxy** [*server-name port*] [**detail**]

Parameter	Description
server-name port	Show statistics for the specified server and port only.
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows summary fast-HTTP-proxy statistics:

```
ACOS# show slb fast-http-proxy
                              Total
-------------------------------------------------------------
----
```

```
Curr Proxy Conns          0
Total Proxy Conns         0
HTTP requests             0
HTTP requests(succ)       0
No proxy error            0
Client RST                0
Server RST                0
No tuple error            0
Parse req fail            0
Server selection fail     0
Fwd req fail              0
Fwd req data fail         0
Req retransmit            0
Req pkt out-of-order      0
Server reselection        0
Server premature close    0
Server conn made          0
Source NAT failure        0
Request over limit        0
Request rate over limit   0
Out RSTs                  0
Full proxy tot            0
Full proxy POST           0
Full proxy pipeline       0
Full proxy fpga err       0
Close on DDoS             0
DNS unresolve             0
Policy drop               0
```

The following table describes the fields in the command output.

Field	Description
Curr Proxy Conns	Number of currently active connections using the fast-HTTP proxy.
Total Proxy Conns	Total number of connections that have used the fast-HTTP proxy.
HTTP requests	Number of HTTP requests received by the fast-HTTP proxy.

Field	Description
HTTP requests (succ)	Number of HTTP requests successfully fulfilled (by establishing a connection to a real server).
No proxy error	Number of proxy errors.
Client RST	Number of times TCP connections with clients were reset.
Server RST	Number of times TCP connections with servers were reset.
No tuple error	Number of tuple errors.
Parse req fail	Number of times the HTTP parser failed to parse a received HTTP request.
Server selection fail	Number of times selection of a real server failed.
Fwd req fail	Number of forward request failures.
Fwd req data fail	Number of forward request data failures.
Req retransmit	Number of retransmitted requests.
Req pkt out-of-order	Number of request packets received from clients out of sequence.
Server reselection	Number of times initial selection of a real server for an HTTP request failed (for example, due to a TCP Reset sent by the server).
Server premature close	Number of times the connection with a server closed prematurely.
Server conn made	Number of connections made with servers.
Source NAT	Number of source NAT failures.

Field	Description
failure	
Request over limit	Number of times the request limit was exceeded.
Request rate over limit	Number of times the request rate limit was exceeded.
Out RSTs	Number of TCP RSTs sent out.
Full proxy tot	Total number of full proxy HTTP sessions.
Full proxy POST	Total number of full proxy sessions for HTTP POST request.
Full proxy pipeline	Total number of pipelined requests.
Full proxy fpga err	Total number of FTA errors.
Close on DDoS	

show slb fix

Description Show SLB statistics for the Financial Information Exchange (FIX) proxy.

Syntax

```
show slb fix [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows FIX SLB statistics.

```
ACOS(config)# show slb fix
                          Total
-------------------------------------------------------------
----
Current proxy conns       4
```

```
Total proxy conns         2
Client fail               7
Server fail               2
Server selection failure  1
no route failure          0
Source NAT failure        1
Insert client IP          5
Default switching         1
Sender ID switching       4
Target ID switching       0
```

The following table describes the fields in the command output.

Field	Description
Current proxy conns	Number of currently active connections using the FIX proxy.
Total proxy conns	Total number of connections that have used the FIX proxy.
Client fail	Number of times that the connection was terminated due to an error on the client side.
Server fail	Number of times that the connection was terminated due to an error on the server side.
Server selection failure	Number of times selection of a real server failed.
no route failure	Number of times FIX failed due to a route lookup failure.
Source NAT Failure	Number of source NAT failures.
Insert client IP	Number of times that the ACOS inserted the client's IP address into tag 11447 and forwarded the recalculated request packet to the FIX server.
Default switching	Number of times that the ACOS parsed the tag value from a client's request and selected a service-group

Field	Description
	based on a match with the configured tag keyword.
Sender ID Switching	Instances of content switching based on the sender's identification tag (SenderCompID).
Target ID Switching	Instances of content switching based on the receiver's identification tag (TargetCompID).

show slb forward-policy-source-port-translation-only-stats

Description Shows or clears the statistics for source port translation only NAT pool instance in the current partition.

Syntax

```
show slb forward-policy-source-port-translation-only-stats

clear slb forward-policy-source-port-translation-only-stats
```

Mode All

Usage The following table describes the fields in the command output:

Field	Description
Group	The IP address used for the NAT mapping.
Port Usage	Number of mappings currently in use by the sessions.
Total Used	Total number of sessions that have been NATed for the source address.
Total Freed	Number of NATed sessions that have been terminated, thus freeing up a port for another session.
Failed	Number of times a mapping attempt failed. Generally, this type of error occurs if the system does not have any resources for new mappings.

Example The following is the example output:

```
ACOS# show slb forward-policy-source-port-translation-only-
stats
Group  Port Usage  Total Used  Total Freed  Failed
```

```
-------------------------------------------------
IPv4    0           0           0           0
IPv6    0           0           0           0
```

show slb ftp

Description Show SLB FTP statistics.

Syntax

```
show slb ftp
```

Mode All

Example The following command shows SLB FTP statistics.

```
ACOS# show slb ftp
Total Control Sessions          0
Total ALG packets               0
ALG packets rexmitted           0
Total Data Sessions             0
Total PORT helper sessions      0
Total PASV helper sessions      0
Drop Data Port out of range     0
```

The following table describes the fields in the command output.

Field	Description
Total Control Sessions	Total number of FTP control sessions load-balanced by the ACOS device.
Total ALG packets	Total number of Application Layer Gateway (ALG) packets.
ALG packets rexmitted	Number of ALG packets that have been retransmitted.
Out of Connections	Number of times an FTP control session could not be established because none of the real servers had available connections.
Total Data Sessions	Total number of FTP data sessions load-balanced by the ACOS device.

Field	Description
Out of Connections	Number of times an FTP data session could not be established because none of the real servers had available connections.

show slb ftp-proxy

Description Display FTP-proxy statistics.

Syntax

```
show slb ftp-proxy [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

show slb generic-proxy

Description Display generic-proxy statistics.

Syntax

```
show slb generic-proxy [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

show slb geo-location

Description Display geo-location information.

Syntax

```
show slb geo-location
[
virtual-server-name |
port-num |
bad-only |
depth  num |
id  group-id |
ip  ipaddr |
```

```
location  location-name |
statistics
]
```

Option	Description
virtual-server-name	Displays geo-location information for only the specified virtual server.
port-num	Displays geo-location information for only the specified virtual port.
bad-only	Displays only the invalid entries.
depth *num*	Specifies how many nodes in the geo-location data tree to display. For example, to display only continent and country entries and hide individual state and city entries, specify depth 2. By default, the full tree is displayed. You can specify 1-5.
id *group-id*	Displays geo-location information for only the specified black/white-list group ID.
ip *ipaddr*	Displays geo-location database entries for only the specified IP address.
location *location-name*	Displays geo-location database entries for only the specified location.
statistics	Displays statistics for the specified geo-location.

Mode All

Example This example displays geo-location statistics

```
ACOS# show slb geo-location statistics

M = Matched or Level, ID = Group ID
Conn = Connection number, Last = Last Matched IP
v = Exact Match, x = Fail
Virtual Server: vip1/80, c-share
-----------------------------------------------------------------
---------
 Max Depth: 3
   Success: 3
```

```
Geo-location                  M   ID Permit     Deny    Conn
Last
-------------------------------------------------------------
---------
US.CA.SJ                      v   3   1          1        1
       77.1.1.107
-------------------------------------------------------------
----------
     Total: 1
```

show slb http-proxy

Description Show statistics for SLB HTTP proxy and EP/TP Proxy

Syntax

```
show slb http-proxy [virtual-server port-num] [detail] | i DOH
```

Option	Description
detail	Lists separate counters for each CPU.
virtual-server port-num	Displays counters for HTTP response codes. For the *virtual-server port-num*, enter the name of a virtual server and its port. The port-num can be 1-65534.

Mode All

Example The following command shows summary HTTP-proxy and EP/TP Proxy statistics:

```
ACOS# show slb http-proxy
                          Total
-------------------------------------------------------------
----
Curr Proxy Conns                      0
Total Proxy Conns                     0
HTTP requests                         0
HTTP requests(succ)                   0
HTTP requests(CONNECT)                0
HTTP requests enter SSLi              0
HTTP req (cache succ)                 0
No proxy error                        0
```

```
Client RST                              0
Server RST                              0
No tuple error                          0
Parse req fail                          0
Server selection fail                   0
Fwd req fail                            0
Fwd req data fail                       0
Req retransmit                          0
Req pkt out-of-order                    0
Server reselection                      0
Server premature close                  0
Server conn made                        0
Source NAT failure                      0
Tot data before compress                0
Tot data after compress                 0
Request over limit                      0
Request rate over limit                 0
Close on DDoS                           0
Tot data pre decompress                 0
Tot data post decompress                0
Status code 1XX                         0
Status code 100                         0
Status code 101                         0
Status code 102                         0
Status code 2XX                         0
..                          0
..                          0
Status code 6XX                         0
Status code unknown                     0
Method GET                              0
Method HEAD                             0
Method PUT                              0
Method POST                             0
Method TRACE                            0
Method TRACK                            0
Method OPTIONS                          0
Method CONNECT                          0
Method DELETE                           0
Method UNKNOWN                          0
Req content len                         0
```

```
Resp content len                    0
Resp chunk encoding                 0
Req <= 1K                           0
............                        0
Req > 256K                          0
Resp <= 1K                          0
............                        0
Resp <= 256K                        0
Resp > 256K                         0
Chunk <= 512                        0
...........                         0
Chunk > 4K                          0
Rsp time < 10u                      0
...............                     0
Rsp time < 100m                     0
Rsp time < 200m                     0
Rsp time < 500m                     0
............                        0
Rsp time >= 5s                      0
```

The following table describes the fields in the command output.

Field	Description
Curr Proxy Conns	Number of currently active HTTP connections using the ACOS device as an HTTP proxy.
Total Proxy Conns	Total number of HTTP connections that have used the ACOS device as an HTTP proxy.
HTTP requests	Total number of HTTP requests received by the HTTP proxy.
HTTP requests (succ)	Number of HTTP requests received by the HTTP proxy that were successfully fulfilled (by connection to a real server).
HTTP requests (CONNECT)	Number of CONNECT requests received by the HTTP proxy.
HTTP requests	Number of HTTP requests directed to SSLi.

Field	Description
enter SSLi	
HTTP req (cache succ)	Number of HTTP requests received by the HTTP proxy that were successfully fulfilled from the cache.
No proxy error	Number of proxy errors.
Client RST	Number of times TCP connections with clients were reset.
Server RST	Number of times TCP connections with servers were reset.
No tuple error	Number of tuple errors.
Parse req fail	Number of times parsing of an HTTP request failed.
Server selection fail	Number of times selection of a real server failed.
Fwd req fail	Number of forward request failures.
Fwd req data fail	Number of forward request data failures.
Req retransmit	Number of retransmitted requests.
Req pkt out-of-order	Number of request packets received from clients out of sequence.
Server reselection	Number of times a request was forwarded to another server because the current server was failing.
Server premature close	Number of times the connection with a server closed prematurely.
Server conn made	Number of connections made with servers.
Source NAT failure	Number of source NAT failures.

Field	Description
Tot data before compress	These counters show statistics for HTTP compression, in bytes before and after commpression.
Tot data after compress	
Request over limit	Number of requests over the limit.
Request rate over limit	Number of requests rate over the limit.
Close on DDoS	Connection was forced to close due to a DDoS attack.
Method *<options>*	Counter for HTTP methods processed, like GET, POST, CONNECT, DELETE and so on.
Response Content Length	Length of Response content in bytes.
Response Chunk Encoding	Encoding statistics for Response compression chunk.
Response Time	**Rsp Time** Response time in seconds.

Example The following command shows HTTP response code statistics:

```
ACOS(config)# show slb http-proxy vs800-http 80
                          Total
-----------------------------------------------------------------
----
status code 1XX           3
status code 2XX           1
status code 3XX           12
status code 4XX           8
status code 5XX           2
status code 6XX           3
...
Rsp time < 200m           0
```

```
Rsp time < 500m          1
Rsp time < 1s            3
Rsp time < 2s            7
Rsp time < 5s            13
Rsp time >= 5s           22

ACOS(config)# show slb http-proxy detail | i DOH
                                                    DP0         DP1
       DP2         Total
-------------------------------------------------------------------
-----------
Curr Proxy Conns                        0           0           0
       0
Total Proxy Conns                       0           0           0
       0
HTTP requests                           0           0           0
       0
HTTP requests(succ)                     0           0           0
       0
HTTP requests(CONNECT)                  0           0           0
       0
HTTP requests enter SSLi                0           0           0
       0
HTTP req (cache succ)                   0           0           0
       0
No proxy error                          0           0           0
       0
Client RST                              0           0           0
       0
Server RST                              0           0           0
       0
No tuple error                          0           0           0
       0
Parse req fail                          0           0           0
       0
Server selection fail                   0           0           0
       0
Fwd req fail                            0           0           0
       0
```

```
Fwd req data fail                       0           0           0
       0
Req retransmit                          0           0           0
       0
Req pkt out-of-order                    0           0           0
       0
Server reselection                      0           0           0
       0
Server premature close                  0           0           0
       0
Server conn made                        0           0           0
       0
Source NAT failure                      0           0           0
       0
Tot data before compress                0           0           0
       0
Tot data after compress                 0           0           0
       0
Request over limit                      0           0           0
       0
Request rate over limit                 0           0           0
       0
Close on DDoS                           0           0           0
       0
Tot data pre decompress                 0           0           0
       0
Tot data post decompress                0           0           0
       0
Status code 1XX                         0           0           0
       0
Status code 100                         0           0           0
       0
Status code 101                         0           0           0
       0
.....

ACOS(config)# show slb http-proxy UDP_VIP 80 | i DOH
DP0         DP1         DP2         Total
```

```
-------------------------------------------------------------------
-----
DOH Req 12
DOH GET Req 6
DOH POST Req 6
DOH Non DOH Req 0
DOH Non DOH GET Req 0
DOH Non DOH POST Req 0
DOH Resp 12
DOH TC Resp 4
DOH UDP DNS Req 12
DOH UDP DNS Resp 8
DOH TCP DNS Req 4
DOH TCP DNS Resp 4
DOH DNS Req Tx Fail 0
DOH DNS Resp Tx Fail 0
DOH Mem Alloc Fail 0
DOH UDP Req Retry 0
DOH UDP Req Retry Fail 0
DOH TCP Req Retry 0
DOH TCP Req Retry Fail 0
DOH Src NAT failed 0
DOH uri path not found 0
DOH GET dns arg failed 0
DOH GET base64 decode failed 0
DOH POST content-type mismatch 0
DOH POST payload not found 0
DOH POST payload extract failed 0
DOH non DOH method 0
DOH TCP send failed 0
DOH UDP send failed 0
DOH Query time out 0
DOH DNS Query type A 16
DOH DNS Query type AAAA 0
DOH DNS Query type NS 0
DOH DNS Query type CNAME 0
DOH DNS Query type ANY 0
DOH DNS Query type SRV 0
DOH DNS Query type MX 0
DOH DNS Query type SOA 0
```

```
DOH DNS Query type Others 0
DOH Resp setup failed 0
DOH Resp header alloc failed 0
DOH Resp Queue failed 0
DOH Resp UDP frag'ed 4
DOH Resp TCP frag'ed 0
DOH Server Select Failed            0
DOH Retry with TCP SG               0

ACOS(config)# show slb http-proxy test-udp 80 detail | i DOH
DP0         DP1         DP2         Total
-------------------------------------------------------------------
----
DOH Req 0 12 12
DOH GET Req 0 6 6
DOH POST Req 0 6 6
DOH Non DOH Req 0 0 0
DOH Non DOH GET Req 0 0 0
DOH Non DOH POST Req 0 0 0
DOH Resp 0 12 12
DOH TC Resp 0 4 4
DOH UDP DNS Req 0 12 12
DOH UDP DNS Resp 0 8 8
DOH TCP DNS Req 0 4 4
DOH TCP DNS Resp 0 4 4
DOH DNS Req Tx Fail 0 0 0
DOH DNS Resp Tx Fail 0 0 0
DOH Mem Alloc Fail 0 0 0
DOH UDP Req Retry 0 0 0
DOH UDP Req Retry Fail 0 0 0
DOH TCP Req Retry 0 0 0
DOH TCP Req Retry Fail 0 0 0
DOH Src NAT failed 0 0 0
DOH uri path not found 0 0 0
DOH GET dns arg failed 0 0 0
DOH GET base64 decode failed 0 0 0
DOH POST content-type mismatch 0 0 0
DOH POST payload not found 0 0 0
DOH POST payload extract failed 0 0 0
DOH non DOH method 0 0 0
```

```
DOH TCP send failed 0 0 0
DOH UDP send failed 0 0 0
DOH Query time out 0 0 0
DOH DNS Query type A 0 16 16
DOH DNS Query type AAAA 0 0 0
DOH DNS Query type NS 0 0 0
DOH DNS Query type CNAME 0 0 0
DOH DNS Query type ANY 0 0 0
DOH DNS Query type SRV 0 0 0
DOH DNS Query type MX 0 0 0
DOH DNS Query type SOA 0 0 0
DOH DNS Query type Others 0 0 0
DOH Resp setup failed 0 0 0
DOH Resp header alloc failed 0 0 0
DOH Resp Queue failed 0 0 0
DOH Resp UDP frag'ed 0 4 4
DOH Resp TCP frag'ed 0 0 0
DOH Server Select Failed 0
DOH Retry with TCP SG 0
```

Field	Description
DOH Req	Total DoH Requests received
DOH GET Req	Total DoH GET Requests received
DOH POST Req	Total DoH POST Requests received
DOH Non DOH Req	Total Non-DoH Requests received with a delay on virtual port bound to virtual port.
DOH Non DOH GET Req	Total Non-DoH GET Requests received on virtual port bound to DOH template.
DOH Non DOH POST Req	Total Non-DoH POST Requests received on virtual port bound to DOH template.
DOH Resp	Total DoH related DNS responses received from backend DNS Server

Field	Description
DOH TC Resp	Total DoH related DNS responses received from backend DNS Server with TC bit set
DOH UDP DNS Req	Total DOH UDP DNS queries sent to backend DNS server
DOH UDP DNS Resp	Total DOH UDP DNS responses received from backend DNS server
DOH TCP DNS Req	Total DOH TCP DNS queries sent to backend DNS server
DOH TCP DNS Resp	Total DOH TCP DNS responses received from backend DNS server
DOH DNS Req Tx Fail	Total DOH DNS Requests failed to be sent out to the backend server
DOH DNS Resp Tx Fail	Total DOH DNS Response failed to be sent out to the client
DOH Mem Alloc Fail	Total Count of DOH related memory allocation failures
DOH UDP Req Retry	Total number of times DOH UDP DNS requests were retried
DOH UDP Req Retry Fail	Total number of times DOH UDP DNS requests retry failed
DOH TCP Req Retry	Total number of times DOH TCP DNS requests were retried
DOH TCP Req Retry Fail	Total number of times DOH TCP DNS requests retry failed
DOH Src NAT failed	Total number of DOH Source NAT Failures
DOH uri path not found	Total count of HTTP requests received not containing DOH URI '/dns-query', when virtual port has DOH template. bound

Field	Description
DOH GET dns arg failed	Total count of HTTP GET requests received not containing a valid arg 'dns=', when virtual port has DOH template. bound
DOH GET base64 decode failed	Total count of HTTP GET requests received where DOH base64url decoding failed, when virtual port has DOH template. bound
DOH POST content-type mismatch	Total count of HTTP POST requests received not containing DOH content-type 'application/dns-message', when virtual port has DOH template. bound
DOH POST payload not found	Total count of HTTP POST requests received not containing payload, when virtual porthas DOH template. bound
DOH POST payload extract failed	Total count of HTTP requests received not containing DOH URI '/DNS-query', when virtual porthas DOH template. bound
DOH non DOH method	Total count of HTTP requests received whose method is not GET or POST, when virtual porthas DOH template. bound
DOH TCP send failed	Total DOH TCP DNS queries failed to be sent out to backend DNS server
DOH UDP send failed	Total DOH UDP DNS queries failed to be sent out to backend DNS server
DOH Query time out	Total DOH DNS queries sent to backend DNS server and timed out due to no response
DOH DNS Query type A	Total DOH requests received containing DNS A query
DOH DNS Query type	Total DOH requests received containing DNS A query

Field	Description
AAAA	
DOH DNS Query type NS	Total DOH requests received containing DNS AAAA query
DOH DNS Query type CNAME	Total DOH requests received containing DNS CNAME query
DOH DNS Query type ANY	Total DOH requests received containing DNS ANY query
DOH DNS Query type SRV	Total DOH requests received containing DNS SRV query
DOH DNS Query type MX	Total DOH requests received containing DNS MX query
DOH DNS Query type SOA	Total DOH requests received containing DNS SOA query
DOH DNS Query type Others	Total DOH requests received containing DNS query type othen than above types
DOH Resp setup failed	Total count of DOH responses failed to be setup
DOH Resp header alloc failed	Total count of header memory allocation failure for DOH responses
DOH Resp Queue failed	Total count of queueing failure for DOH responses to be sent to the client
DOH Resp UDP frag'ed	Total fragmented DOH UDP DNS responses received from backend DNS server
DOH Resp	Total fragmented DOH TCP DNS responses received

Field	Description
TCP frag'ed	from backend DNS server
DOH Server Select Failed	Total number of times backend dns server selection failed for DOH
DOH Retry with TCP SG	Total number of times DOH attempted to retry with backend TCP DNS service-group after connecting to UDP DNS Servers failed

show slb http3

Description Shows the SLB HTTP/3 statistics.

Syntax

```
show slb http3
```

Mode All

Example The following command shows the SLB HTTP/3 statistics.

```
ACOS# show slb http3
```

```
                                                                Total
-----------------------------------------------------------------------
--
Current HTTP/3 Client Connections                                   1
Current HTTP/3 Server Connections                                   1
Total HTTP/3 Client Connections                                     5
Total HTTP/3 Server Connections                                     6
Peak HTTP/3 Client Connections                                      0
Peak HTTP/3 Server Connections                                      0
Current Request Streams on client side                              0
Current Request Streams on server side                              0
Total Request Streams on client side                                0
Total Request Streams on server side                                0
Current Push Streams on client side                                 0
Current Push Streams on server side                                 0
Total Push Streams on client side                                   0
Total Push Streams on server side                                   0
Current Other Streams on client side                                0
Current Other Streams on server side                                0
Total Other Streams on client side                                  0
Total Other Streams on server side                                  0
HEADERS Frame received on client side                               0
HEADERS Frame sent on client side                                   0
DATA Frame received on client side                                  0
DATA Frame sent on client side                                      0
CANCEL PUSH Frame received on client side                           0
CANCEL PUSH Frame sent on client side                               0
SETTINGS Frame received on client side                              0
SETTINGS Frame sent on client side                                  0
PUSH PROMISE Frame received on client side                          0
PUSH PROMISE Frame sent on client side                              0
GOAWAY Frame received on client side                                0
GOAWAY Frame sent on client side                                    0
MAX PUSH ID Frame received on client side                           0
MAX PUSH ID Frame sent on client side                               0
Unknown Frame received on client side                               0
HEADER Frames passed to HTTP layer on client side                   0
DATA Frames passed to HTTP layer on client side                     0
```

Bytes received in HEADER frames on client side	0
Bytes sent in HEADER frames on client side	0
Bytes received in DATA frames on client side	0
Bytes sent in DATA frames on client side	0
Bytes received in other frames on client side	0
Bytes sent in other frames on client side	0
Bytes received in heading on client side	0
Bytes sent in heading on client side	0
Total Bytes received on client side	0
Total Bytes sent on client side	0
HEADERS Frame received on server side	0
HEADERS Frame sent on server side	0
DATA Frame received on server side	0
DATA Frame sent on server side	0
CANCEL PUSH Frame received on server side	0
CANCEL PUSH Frame sent on server side	0
SETTINGS Frame received on server side	0
SETTINGS Frame sent on server side	0
PUSH PROMISE Frame received on server side	0
PUSH PROMISE Frame sent on server side	0
GOAWAY Frame received on server side	0
GOAWAY Frame sent on server side	0
MAX PUSH ID Frame received on server side	0
MAX PUSH ID Frame sent on server side	0
Unknown Frame received on server side	0
HEADER Frames passed to HTTP layer on server side	0
DATA Frames passed to HTTP layer on server side	0
Bytes received in HEADER frames on server side	0
Bytes sent in HEADER frames on server side	0
Bytes received in DATA frames on server side	0
Bytes sent in DATA frames on server side	0
Bytes received in other frames on server side	0
Bytes sent in other frames on server side	0
Bytes received in heading on server side	0
Bytes sent in heading on server side	0
Total Bytes received on server side	0
Total Bytes sent on server side	0
Invalid Argument	0

```
Invalid State                                0
Wouldblock                                   0
Stream In Use                                0
Push Id Blocked                              0
Malformed Http Header                        0
Remove Http Header                           0
Malformed Http Messaging                     0
Too Late                                     0
Qpack Fatal                                  0
Qpack Header Too Large                       0
Ignore Stream                                0
Stream Not Found                             0
Ignore Push Promise                          0
Qpack Decompression Failed                   0
Qpack Encoder Stream Error                   0
Qpack Decoder Stream Error                   0
H3 Frame Unexpected                          0
H3 Frame Error                               0
H3 Missing Settings                          0
H3 Internal Error                            0
H3 Closed Critical Stream                    0
H3 General Protocol Error                    0
H3 Id Error                                  0
H3 Settings Error                            0
H3 Stream Creation Error                     0
Fatal Error                                  0
HTTP/3 Connection Allocation Error           0
Memory Allocation Failures                   0
HTTP3 Rejected                               0
```

The following table describes the fields in the command output.

Counters	Description
Current HTTP/3 Client Connections	Displays the number of current HTTP/3 client connections.
Current HTTP/3 Server Connections	Displays the number of current HTTP/3 server connections.

Counters	Description
Total HTTP/3 Client Connections	Displays the total number of HTTP/3 client connections.
Total HTTP/3 Server Connections	Displays the total number of HTTP/3 server connections.
Peak HTTP/3 Client Connections	Displays the number of peak HTTP/3 client connections.
Peak HTTP/3 Server Connections	Displays the number of peak HTTP/3 server connections.
Current Request Streams on client side	Displays the number of current HTTP/3 request steam sessions on the client side.
Current Request Streams on server side	Displays the number of current HTTP/3 request steam sessions on the server side.
Total Request Streams on client side	Displays the total number of HTTP/3 request stream sessions on the client side.
Total Request Streams on server side	Displays the total number of HTTP/3 request stream sessions on the server side.
Current Push Streams on client side	Displays the number of HTTP/3 push stream sessions on the client side.
Current Push Streams on server side	Displays the number of HTTP/3 push stream sessions on the server side.
Total Push Streams on client side	Displays the total number of HTTP/3 push stream sessions on the client side.
Total Push Streams on server side	Displays the total number of HTTP/3 push stream sessions on the client side.
Current Other Streams on client side	Displays the number of other HTTP/3 stream sessions on the client side.
Current Other Streams on server side	Displays the number of other HTTP/3 stream sessions on the server side.
Total Other Streams on client side	Displays the total number of other HTTP/3 stream sessions on the client side.
Total Other Streams	Displays the total number of other HTTP/3

Counters	Description
on server side	stream sessions on the server side.
HEADERS Frame received on client side	Displays the number of various header frames received and sent on the client side.
HEADERS Frame sent on client side	
DATA Frame received on client side	
DATA Frame sent on client side	
CANCEL PUSH Frame received on client side	
CANCEL PUSH Frame sent on client side	
SETTINGS Frame received on client side	
SETTINGS Frame sent on client side	
PUSH PROMISE Frame received on client side	
PUSH PROMISE Frame sent on client side	
GOAWAY Frame received on client side 0	
GOAWAY Frame sent on client side	
MAX PUSH ID Frame received on client side	
MAX PUSH ID Frame sent on client side	
Unknown Frame	

Counters	Description
received on client side 0	
HEADER Frames passed to HTTP layer on client side 0	
DATA Frames passed to HTTP layer on client side	
Bytes received in HEADER frames on client side 0	
Bytes sent in HEADER frames on client side	
Bytes received in DATA frames on client side	
Bytes sent in DATA frames on client side	
Bytes received in other frames on client side	
Bytes sent in other frames on client side	
Bytes received in heading on client side	Displays the number of bytes received and sent in the heading on the client side.
Bytes sent in heading on client side	
Total Bytes received on client side	Displays the total number of bytes received and sent in the heading on the client side.
Total Bytes sent on client side	
HEADERS Frame received on server side	Displays the number of various header frames received and sent on the server

Counters	Description
	side.

Counters	Description
HEADERS Frame sent on server side	
DATA Frame received on server side	
DATA Frame sent on server side 0	
CANCEL PUSH Frame received on server side	
CANCEL PUSH Frame sent on server side	
SETTINGS Frame received on server side	
SETTINGS Frame sent on server side	
PUSH PROMISE Frame received on server side	
PUSH PROMISE Frame sent on server side	
GOAWAY Frame received on server side	
GOAWAY Frame sent on server side	
MAX PUSH ID Frame received on server side	
MAX PUSH ID Frame sent on server side	
Unknown Frame received on server side	
HEADER Frames passed to HTTP layer on server side	

Counters	Description
DATA Frames passed to HTTP layer on server side	
Bytes received in HEADER frames on server side	
Bytes sent in HEADER frames on server side	
Bytes received in DATA frames on server side	
Bytes sent in DATA frames on server side	
Bytes received in other frames on server side	
Bytes sent in other frames on server side	
Bytes received in heading on server side	Displays the number of bytes received and sent in the heading on the server side.
Bytes sent in heading on server side	
Total Bytes received on server side	Displays the total number of bytes received and sent in the heading on the server side.
Total Bytes sent on server side	
Invalid Argument	Displays the number of invalid arguments in the HTTP/3 status code.
Invalid State	Displays the number of invalid states in the HTTP/3 status code.
Wouldblock	Displays the number of wouldblock status code.
Stream In Use	Displays the number of STREAM in use.

Counters	Description
Push Id Blocked	Displays the number PUSH ID blocked.
Malformed Http Header	Displays the number of HTTP headers that were malformed.
Remove Http Header	Displays the number of HTTP headers that were removed.
Malformed Http Messaging	Displays the number of malformed HTTP message.
Ignore Stream	Displays the number of STREAMs that were ignored.
Stream Not Found	Displays the number of STREAMs that were not found.
Ignore Push Promise	Displays the number of PUSH_PROMISE frames that were ignored.
Too Late	
Qpack Fatal	Displays the QPACK header compression-specific statistics. Like HPACK in HTTP/2, QPACK is a compression format for efficiently representing the HTTP fields in HTTP/3.
Qpack Header Too Large	
Qpack Decompression Failed	
Qpack Encoder Stream Error	
Qpack Decoder Stream Error	

Counters	Description
H3 Frame Unexpected	Displays various error statistics in HTTP/3 connection.
H3 Frame Error	
H3 Missing Settings	
H3 Internal Error	
H3 Closed Critical Stream	
H3 General Protocol Error	
H3 Id Error	
H3 Settings Error	
H3 Stream Creation Error	
Fatal Error	
HTTP/3 Connection Allocation Error	
Memory Allocation Failures	
HTTP3 Rejected	

show slb hw-compression

Description Show statistics for hardware-based compression.

Syntax

```
show slb hw-compression [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Usage Hardware-based compression is available using an optional hardware module in some models. If this command does not appear on your ACOS device, the device does not contain a compression module.

Example The following commands first enable hardware-based compression (**hw-compression** command), then display statistics for the feature:

```
ACOS(config)# slb common
ACOS(config-common)# hw-compression
ACOS(config-common)# show slb hw-compression
Hardware compression device is installed.
Hardware compression module is enabled.
                          Total
-------------------------------------------------------------
----
total request count       177157
total submit count        177157
total response count      177157
total failure count       0
last failure code         0
compression queue full    0
max queued request count 84
max queued submit count  68
```

show slb icap

Description Show ICAP statistics for debugging.

Syntax

```
show slb icap [detail]
```

Mode All

Example The following command shows ICAP statistics:

```
ACOS# show slb icap detail
                           DP0     DP1    DP2    DP3    DP4    DP5
Total
-------------------------------------------------------------
----
reqmod request              0       0      0      0      0      0
 0
respmod request             0       0      0      0      0      0
 0
reqmod req after 100        0       0      0      0      0      0
 0
```

```
respmod req after 100       0       0       0       0       0       0
 0
reqmod response             0       0       0       0       0       0
 0
respmod response            0       0       0       0       0       0
 0
reqmod resp after 100       0       0       0       0       0       0
 0
respmod resp after 100      0       0       0       0       0       0
 0
send option req             0       0       0       0       0       0
 0
recv option resp            0       0       0       0       0       0
 0
http connect reqmod request0        0       4       0       0       0
 4
chunk no allow 204          0       0       0       0       0       0
 0
Big CL so no allow 204      0       0       0       0       0       0
 0
result continue             0       0       0       0       0       0
 0
result icap response        0       0       0       0       0       0
 0
result 100 continue         0       0       0       0       0       0
 0
result other                0       0       0       0       0       0
 0
status 2xx                  0       0       0       0       0       0
 0
status 200                  0       0       0       0       0       0
 0
status 201                  0       0       0       0       0       0
 0
status 202                  0       0       0       0       0       0
 0
.......
status unknown              0       0       0       0       0       0
 0
```

```
app serv conn no pcb err    0       0       0       0       0       0
 0
app serv conn err           0       0       0       0       0       0
 0
chunk1 hdr err              0       0       0       0       0       0
 0
chunk2 hdr err              0       0       0       0       0       0
 0
chunk bad trail err         0       0       0       0       0       0
 0
no payload next buff err    0       0       0       0       0       0
 0
no payload buff err         0       0       0       0       0       0
 0
resp hdr incomplete err     0       0       0       0       0       0
 0
serv sel fail err           0       0       0       0       0       0
 0
start icap conn fail err    0       0       0       0       0       0
 0
prep req fail err           0       0       0       0       0       0
 0
icap ver err                0       0       0       0       0       0
 0
icap line err               0       0       0       0       0       0
 0
encap hdr incomplete err    0       0       0       0       0       0
 0
no icap resp err            0       0       0       0       0       0
 0
resp line read err          0       0       0       0       0       0
 0
...
```

show slb icap-http

Description Show ICAP HTTP statistics for debugging.

Syntax

```
show slb icap-http [detail]
```

Mode All

Example The following command shows SYN-cookie statistics:

```
ACOS# show slb icap-http detail
            DP0

DP1

DP2

DP3
 DP4 DP5 DP6 DP7 DP8 DP9 DP10 DP11 DP12 DP13 DP14 DP15 Total
----------------------------------------
status
2xx

0

0

0

0   0   0   0   0   0   0    0    0    0    0    0    0    0
status 200    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 201    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 202    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 203    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 204    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 205    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 206    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
status 207    0   0   0   0   0   0   0   0   0   0    0    0
  0    0    0    0    0
```

```
status 1xx     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 100     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 101     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 102     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 3xx     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 300     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 301     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 302     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 303     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 304     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 305     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 306     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 307     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 4xx     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 400     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 401     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 402     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 403     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 404     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
```

```
status 405    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 406    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 407    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 408    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 409    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 410    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 411    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 412    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 413    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 414    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 415    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 416    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 417    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 418    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 419    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 422    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 423    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 424    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
status 425    0   0   0   0   0   0   0   0   0   0   0   0
  0    0    0    0    0
```

```
status 426     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 449     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 450     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 5xx     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 500     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 501     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 502     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 503     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 504     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 505     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 506     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 507     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 508     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 509     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 510     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
status 6xx     0    0    0    0    0    0    0    0    0    0    0    0
  0     0     0     0     0
```

show slb imap-proxy

Description Displays the IMAP proxy statistics.

Syntax

```
show slb imap-proxy
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb imap-proxy
                                        Total
-----------------------------------------------
Current proxy conns                         0
Total proxy conns                           0
Total IMAP Request                          0
Server selection failure                    0
no route failure                            0
source nat failure                          0
start tls cmd                               0
Login Pakcet                                0
capability packet                           0
request line freed                          0
invalid start line                          0
other cmd                                   0
line too long                               0
Control chn ssl                             0
Bad Sequence                                0
Serv Sel Persist fail                       0
Serv Sel SMPv6 fail                         0
Serv Sel SMPv4 fail                         0
Serv Sel ins tpl fail                       0
Client EST state err                        0
Serv CTNG state err                         0
Serv RESP state err                         0
Client RQ state err                         0
Realloc error                               0
Alloc error                                 0
Boundary error                              0
Negative_error                              0
```

Field	Description
`Current proxy conns`	Number of currently active IMAP proxy connections.

Field	Description
Total proxy conns	Total number of IMAP proxy connections.
Total IMAP Request	Total number of IMAP requests processed by the proxy.
Server selection failure	Number of times server selection failured.
no route failure	Number of instances where no route was found.
source nat failure	Number of times source NAT failured.
start tls cmd	Number of times STARTTLS command was processed.
Login Packet	Number of IMAP login packets processed.
capability packet	Number of IMAP capability packets processed.
request line freed	Number of request lines freed.
invalid start line	Number of invalid start lines detected.
other cmd	Number of other IMAP commands processed.
line too long	Number of times the request line was too long.
Control chn ssl	Number of SSL connections established for the control channel.
Bad Sequence	Number of times IMAP command were out of order.
Serv Sel Persist fail	Number of server selection failures due to persistence settings.
Serv Sel SMPv6 fail	Number of server selection SMPv6 failures.
Serv Sel SMPv4 fail	Number of server selection SMPv4 failures.
Serv Sel ins tpl fail	Number of server selection failures due

Field	Description
	to insertion template.
Client EST state err	Number of client established state errors.
Serv CTNG state err	Number of server CTNG state errors.
Serv RESP state err	Number of server response state errors.
Client RQ state err	Number of client request state errors.
Realloc error	Number of errors during memory reallocation.
Alloc error	Number of errors during memory allocation .
Boundary error	Number of boundary errors.
Negative_error	Number of negative errors.

show slb l4

Description Show Layer-4 SLB statistics.

Syntax

```
show slb l4 [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows summary statistics for Layer 4 SLB:

```
ACOS# show slb l4
                          Total
-------------------------------------------------------------
----
IP out noroute            0
TCP out RST               0
TCP out RST no SYN        0
TCP out RST L4 proxy      0
TCP out RST ACK attack    0
TCP out RST aFleX         0
```

```
TCP out RST stale sess   0
TCP out RST TCP proxy    0
TCP SYN received         226510
TCP SYN cookie snt       226510
TCP SYN cookie expd snt  0
TCP SYN cookie snt fail  0
TCP received             1042844
UDP received             0
L2 DSR received          0
L3 DSR received          0
Server sel failure       0
Source NAT failure       0
Source NAT no fwd route  0
Source NAT no rev route  0
Source NAT ICMP Process  0
Source NAT ICMP No Match 0
Auto NAT id mismatch     0
TCP SYN cookie failed    0
L4 SYN attack            226510
NAT no session drops     0
virtual portnot matching drops 0
No SYN pkt drops         0
No SYN pkt drops - FIN   0
No SYN pkt drops - RST   0
No SYN pkt drops - ACK   0
Conn Limit drops         0
Conn Limit resets        0
Conn rate limit drops    0
Conn rate limit resets   0
Proxy no sock drops      0
PROXY protocol header inserted 0
PROXY protocol header retransmitted 0
PROXY protocol error     0
PROXY protocol drop      0
aFleX drops              0
Session aged out         0
TCP Session aged out     0
UDP Session aged out     0
Other Session aged out   0
TCP no SLB               0
```

```
UDP no SLB                0
SYN Throttle              0
Inband HM retry           0
Inband HM reassign        0
Auto-reselect server      0
Fast aging set            0
Fast aging reset          0
TCP invalid drop          0
Out of sequence ACK drop 0
SYN stale sess drop       589824
Anomaly out of sequence   0
Anomaly zero window       0
Anomaly bad content       0
Anomaly pbslb drop        0
No resource drop          0
Reset unknown conn        0
RST L7 on failover        0
TCP SYN Other Flags Drop 0
TCP SYN With Data Drop    0
ignore msl                0
NAT Port Preserve Try     0
NAT Port Preserve Succ    0
BW-Limit Exceed drop      0
BW-Watermark drop         0
L4 CPS exceed drop        0
NAT CPS exceed drop       0
L7 CPS exceed drop        0
SSL CPS exceed drop       0
SSL TPT exceed drop       0
SSL TPT-Watermark drop    0
L3V Conn Limit Drop       0
L4 server handshake fail 0
L4 AX re-xmit SYN         0
L4 rcv ACK on SYN         0
L4 rcv RST on SYN         0
TCP no-Est Sess aged out 0
no-Est CSYN rcv aged out 0
no-Est SSYN snt aged out 0
L4 rcv rexmit SYN         589824
L4 rcv rexmit SYN (delq) 589824
```

```
L4 rcv rexmit SYN|ACK    0
L4 rcv rexmit SYN|ACK DQ 0
L4 rcv fwd last ACK      0
L4 rcv rev last ACK      0
L4 rcv fwd FIN           0
L4 rcv fwd FIN dup       0
L4 rcv fwd FIN|ACK       0
L4 rcv rev FIN           0
L4 rcv rev FIN dup       0
L4 rcv rev FIN|ACK       0
L4 rcv fwd RST           226510
L4 rcv rev RST           0
L4 UDP reqs no rsp       0
L4 UDP req rsps          0
L4 UDP req/rsp not match 0
L4 UDP req > rsps        0
L4 UDP rsps > reqs       0
L4 UDP reqs              0
L4 UDP rsps              0
L4 TCP Established       0
Skip Insert-client-ip    0
DNS query id switch      0
```

The following table describes the fields in the command output.

Field	Description
IP out noroute	Number of IP packets that could not be routed. These packets are dropped by the ACOS device.
TCP out RST	Number of TCP Resets sent.
TCP out RST no SYN	Number of Resets sent for which there was no SYN.
TCP out RST L4 proxy	Number of TCP Reset packets the ACOS device has sent as a Layer 4 proxy.
TCP out RST ACK attack	Number of TCP Resets sent in response to a TCP ACK attack.
TCP out RST aFleX	Number of TCP Reset packets the ACOS device has sent due to an aFleX policy.

Field	Description
TCP out RST stale sess	This counter is incremented each time the following occurs: • A client SYN is received • "reset on terminated session SYN packet" is enabled in the delete queue (this is enabled by default) • "slb reset-stale-session" is enabled. In such cases, an RST is sent out and the counter is incremented.
TCP out RST TCP proxy	Number of TCP Reset packets the ACOS device has sent as a TCP proxy.
TCP SYN received	Number of first SYN packets the ACOS device has received from the client.
TCP SYN cookie snt	Number of TCP SYN cookies sent.
TCP SYN cookie expd snt	Number of TCP SYN cookies with expanded options that were sent. **NOTE:** Expanded SYN cookie options are disabled by default but can be enabled using syn-cookie command.
TCP SYN cookie snt fail	Number of TCP SYN cookie send attempts that failed because delivery to the client failed.
TCP received	Number of subsequent packets ACOS received from a client during a particular session. Counter includes the following types of packets: SA, A, FINACK, PSHACK.
UDP received	Number of UDP packets received.
L2 DSR received	Number of reply packets received for Layer 2 DSR sessions.
L3 DSR	Number of reply packets received for Layer 3 DSR

Field	Description
received	sessions.
Server sel failure	Number of times selection of a real server failed.
Source NAT failure	Number of times a source NAT failure occurred.
Source NAT no fwd route	Number of times there was no route to the destination for Layer 3 NAT traffic.
Source NAT no rev route	Number of times there was no route to the source for Layer 3 NAT traffic.
Source NAT ICMP Process	Number of times an ICMP error related to source NAT occurred.
Source NAT ICMP No Match	Number of times an ICMP error related to source NAT occurred, and there was no matching session for the traffic.
Auto NAT ID mismatch	Number of times a mismatch has occurred between a Smart NAT resource and a VRRP-A VRID.
TCP SYN cookie failed	Number of times a TCP SYN cookie validate failure occurred when the client never sent an ACK packet to complete the TCP three-way handshake.
L4 SYN attack	Total number of TCP SYNs received by the ACOS device that were not followed by a valid client ACK to establish the connection. This counter is calculated as follows: `(Total-SYNs-Received-by-Hardware + Total-SYNs-Received-by-Software) - Total-Number-of-Successful-Connections = L4-SYN-Attack-Count`
NAT no session drops	Number of packets sent to the NAT Pool IP, but for which there was no corresponding session on the device.

Field	Description
virtual portnot matching drops	Number of packets received on a virtual port that was either down, disabled, or non-existent.
No SYN pkt drops	The cumulative number of the following three types of packets: ACK, RST, FIN.
No SYN pkt drops - FIN	Number of FIN packets received for which there was no corresponding session on the ACOS device.
No SYN pkt drops - RST	Number of RST packets received for which there was no corresponding session on the ACOS device.
No SYN pkt drops - ACK	Number of ACK packets received for which there was no corresponding session on the ACOS device.
Conn Limit drops	Number of connections dropped because the server connection limit had been reached.
Conn Limit resets	Number of connections reset because the server connection limit had been reached.
Conn rate limit drops	Number of connections dropped by connection rate limiting.
Conn rate limit resets	Number of connections reset by connection rate limiting.
Proxy no sock drops	Number of packets dropped because the proxy did not have an available socket.
PROXY protocol header inserted	Number of headers inserted. It can only be increased once per connection.
PROXY protocol header retransmitted	Number of headers retransmitted.
PROXY protocol error	Number of internal errors occurred when processing the proxy protocol header connection.

Field	Description
PROXY protocol drop	Number of packets dropped when processing the proxy protocol header connection.
aFleX drops	Number of packets dropped due to an aFleX policy.
Session aged out	Total number of TCP (TCP Session aged out), UDP (UDP Session aged out) and other (Other session aged out) sessions that aged out.
TCP Session aged out	Number of TCP sessions that aged out, including both half-open and established sessions.
UDP Session aged out	Number of UDP sessions that have aged out.
Other Session aged out	Number of sessions of other types (not TCP or UDP) that have aged out.
TCP no SLB	This counter is deprecated and is no longer used.
UDP no SLB	Number of non-SLB UDP packets received by the ACOS device.
SYN Throttle	If the count of buffers allocated from system memory is higher than currently available free system buffers, a flag is enabled to 'throttle SYN'. For TCP connections, this means that incoming packets for new TCP connections are dropped to avoid queuing more buffers for processing.
Inband HM retry	Number of times the ACOS device retried an inband health check, because a SYN-ACK was not received for the previous SYN.
Inband HM reassign	Number of times the ACOS device reassigned a client's traffic to another server, because the initial server exceeded the maximum number of retries allowed by the inband health check.
Auto-reselect server	Number of times the ACOS device has reperformed server selection automatically because the initially selected server did not respond to the TCP-SYN from the ACOS device.

Field	Description
	NOTE: Starting with ACOS 5.2.1-P2, this counter works on TCP virtual ports other than HTTP/HTTPS (like tcp-proxy, tcp and so on).
Fast aging set	Number of times fast aging of idle connections was automatically enabled by the ACOS device due to factors such as low availability of I/O buffers, number of sessions or amount of available memory.
Fast aging reset	Number of times fast aging of idle connections was disabled. This occurs after a sufficient number of buffers become available again.
TCP invalid drop	Number of TCP packets received by the ACOS device that did not conform to the standard format for TCP packets. For example, this counter is incremented if the ACOS device receives a packet whose total length is less than the following: Internet-Header-Length * 4 + TCP-data-offset *4
Out of sequence ACK drop	Number of TCP ACKs that were dropped because they were out of sequence.
SYN stale sess drop	This counter is incremented each time the following occurs: • A client SYN is received • “reset on terminated session SYN packet” is enabled in the delete queue (this is enabled by default) • “slb reset-stale-session” is disabled. In such cases, the packet is dropped and the counter is incremented.
Anomaly out of sequence	Number of packets that matched an IP anomaly out-of-sequence filter.

Field	Description
	NOTE: To configure IP anomaly filters, see the **`ip anomaly-drop`** command.
Anomaly zero window	Number of packets that matched an IP anomaly zero-window filter.
Anomaly bad content	Number of packets that matched an IP anomaly bad-content filter.
Anomaly PBSLB drop	Number of packets that matched an IP anomaly filter used for system-wide Policy-Based SLB (PBSLB).
No resource drop	Number of times traffic has been dropped because the ACOS device had run out of Layer 4 session resources.
Reset unknown conn	Number of times the ACOS device sent a RST in response to a non-SYN packet for a non-existent session. **NOTE:** This feature is enabled using the **`reset-unknown-conn`** option in slb template virtual-port.
RST L7 on failover	Number of Layer 7 sessions that were reset following VRRP-A failover.
TCP SYN Other Flags Drop	Number of TCP SYN packets that were dropped by the ACOS device because they contained a flag other than the SYN flag.
TCP SYN With Data Drop	Number of TCP SYN packets that were dropped by the ACOS device because they contained data.
Ignore MSL	Number of times a SYN packet reaches the MSL limit (default is 2 seconds) during a time-wait state and does not get dropped due to the “ignore-tcp-msl” option being configured in the slb template virtual-port.
NAT Port	Number of times the client port preservation

Field	Description
Preserve Try	feature attempted to preserve a client's source port for traffic destined to a virtual port. **NOTE:** This feature is enabled using the snat-port-preserve option in the slb template virtual-port.
NAT Port Preserve Succ	Number of times the client port preservation feature successfully preserved a client's source port for traffic destined to a virtual port.
BW-Limit Exceed drop	Number of times traffic was dropped because a configured bandwidth limit was exceeded.
BW-Watermark drop	Number of times traffic was dropped because a configured bandwidth watermark was exceeded.
L4 CPS exceed drop	Number of times traffic was dropped because the maximum allowed number of Layer 4 connections per second (CPS) was exceeded.
NAT CPS exceed drop	Number of times traffic was dropped because the maximum allowed number of NAT CPS was exceeded.
L7 CPS exceed drop	Number of times traffic was dropped because the maximum allowed number of Layer 7 CPS was exceeded.
SSL CPS exceed drop	Number of times traffic was dropped because the maximum allowed number of SSL CPS was exceeded.
SSL TPT exceed drop	Number of times SSL traffic was dropped because SSL throughput exceeded the maximum allowed by a system-resource template.
SSL TPT-Watermark drop	Number of times SSL traffic was dropped because SSL throughput exceeded the configured watermark.

Field	Description
L3V Conn Limit Drop	Number of times Layer 3 traffic was dropped because a configured connection limit was exceeded.
L4 server handshake fail	Number of times traffic was dropped because the Layer 4 handshake with a server failed.
L4 AX re-xmit SYN	Number of times the ACOS device needed to retransmit a TCP SYN.
L4 rcv ACK on SYN	Number of SYN-ACKs (ACKs in response to TCP-SYNs) received by the ACOS device.
L4 rcv RST on SYN	Number of TCP Resets (RST) the ACOS device received in response to a SYN.
TCP no-Est Sess aged out	Number of half-open sessions on the ACOS device. A half-open session means the ACOS device received a SYN packet, forwarded it to the backend server but there was no SYN-ACK from the backend server, resulting in a half-open session on the ACOS device. These sessions are created with a session age time of 60 seconds. If the session is idle for more than 60 seconds, ACOS terminates the session and removes it from the session table and increments this counter.
no-Est CSYN rcv aged out	Number of times the ACOS device received a SYN from a client and forwarded it to the server. This can create a half-open session on the ACOS device if there is no SYN-ACK from the server for a period exceeding 60 seconds. If this happens, ACOS kills the session and increments this counter.
no-Est SSYN snt aged out	Number of TCP sessions that aged out before a SYN was received from the server, and therefore could not be established.
L4 rcv rexmit SYN	Number of times the client does not get a SYN-ACK from the server. This causes the client to retransmit same SYN packet that it sent earlier. This counter

Field	Description
	will increment each time such a re-transmission of the SYN packet occurs.
L4 rcv rexmit SYN (delq)	Number of times the client SYN packet matches an existing session currently in the delete queue. When this occurs, both the “L4 rcv rexmit SYN” and “L4 rcv rexmit SYN (delq)” counters are incremented.
L4 rcv rexmit SYN|ACK	Total number of retransmitted SYN-ACKs received by the ACOS device.
L4 rcv rexmit SYN|ACK DQ	Number of retransmitted SYN-ACKs received by the ACOS device for sessions that had already been moved to the delete queue.
L4 rcv fwd last ACK	Number of final ACKs (last ACKs of a given TCP session) received by the ACOS device from clients. **NOTE:** In this field and the following fields, the following terms describe the traffic origination and direction: • rcv fwd – Final ACKs received from the client. • rcv rev – Final ACKs received from the server.
L4 rcv rev last ACK	Number of final ACKs (last ACKs of a given TCP session) received by the ACOS device from servers.
L4 rcv fwd FIN	Number of TCP FINs received from clients.
L4 rcv fwd FIN dup	Number of times more than one FIN packet is received from the client. An example of this would be if the server did not reply to a FIN-ACK in time, thus causing the client to send another FIN.

Field	Description
L4 rcv fwd FIN|ACK	Number of TCP FIN-ACKs received from clients.
L4 rcv rev FIN	Number of TCP FINs received from servers.
L4 rcv rev FIN dup	Number of duplicate TCP FINs received from servers.
L4 rcv rev FIN|ACK	Number of TCP FIN-ACKs received from servers.
L4 rcv fwd RST	Number of TCP RST packets that the ACOS device received from a client and forwarded to the server.
L4 rcv rev RST	Number of TCP RST packets that the ACOS device received from a server and forwarded to the client.
L4 UDP reqs no rsp	Number of port 53 UDP requests received to which there was no response.
L4 UDP req rsps	Number of port 53 UDP requests received to which there was a response.
L4 UDP req/rsp not match	Number of mismatches between port 53 UDP requests and responses.
L4 UDP req > rsps	Number of port 53 UDP requests received for which there was no corresponding response.
L4 UDP rsps > reqs	Number of port 53 UDP responses received for which there was no corresponding request.
L4 UDP reqs	Total number of port 53 UDP requests received by the ACOS device.
L4 UDP rsps	Total number of port 53 UDP responses received by the ACOS device.
L4 TCP Established	Number of established sessions that completed a 3-way TCP handshake.
Skip Insert-client-ip	Number of times client IP insertion into TCP option failed due to lack of space.
DNS query id switch	Number of requests load balanced based on DNS query ID.

show slb l7session

Description Displays Layer 7 (L7) session statistics for each data plane.

Syntax `show slb l7session [detail]`

Option	Description
detail	Display detailed information of each counter.

Mode All

Example The following example displays sample output:

```
ACOS# show slb l7session
                                        Total
-----------------------------------------------
Curr proxy conn                           0
Total proxy conn                          0
Start server conn success                 0
Server selection fail                     0
Server connection fail                    0
Data event from TCP                       0
Data event from UDP                       0
Data event callback fail                  0
Err event from TCP                        0
Err event callback fail                   0
FIN from client                           0
FIN from server                           0
RST from client                           0
RST from server                           0
Fwd req fail                              0
```

Field	Description
Curr proxy conn	Number of current active L7 proxy connections.
Total proxy conn	Total number of L7 proxy connections.
Start server conn	Number of successful server connection

Field	Description
success	starts.
Server selection fail	Number of server selection failures.
Server connection fail	Number of server connection failures.
Data event from TCP	Number of data events received from TCP layer.
Data event from UDP	Number of data events received from UDP layer.
Data event callback fail	Number of data event callback failures.
Err event from TCP	Number of error events received from TCP.
Err event callback fail	Number of error event callback failures.
FIN from client	Number of FIN packets received from the client.
FIN from server	Number of FIN packets received from the server.
RST from client	Number of RST packets received from the client.
RST from server	Number of RST packets received from the server.
Fwd req fail	Number of failures occurred while forwarding requests.

show slb link-probe

Description Display options for the show slb link-probe command.

Syntax

```
show slb link-probe {entry | statistics} [server [<server_name> |<service_group_name>] detail]
```

Parameter	Description
entry	Display link probe entries. Display statistics for information about SLB link-probe entries currently created in the system.
statistics	Display all link probe statistics.
server *<server_name>*	Display information about slb link-probe entries currently created in the system associated with a specific server.
<service_group_name>	Display information about slb link-probe entries currently created in the system associated with a specific service-group
detail	Display detailed information about slb link-probe entries currently created in the system associated with a specific server or service-group.

Default NA

Mode All

Example

```
ACOS(config)# show slb link-probe entry

   Next-Hop SLB Server       IP Type       Probe Dest IP
Address            Domain-Name                      URL
     Average RTT
-------------------------------------------------------------
-------------------------rs212                         Static
  172.16.213.93               test1.example.com           /
                            33


-------------------------------------------------------------
------------------------- Next-Hop SLB Server       IP Type
   Probe Dest IP Address            Domain-Name
     URL              Average RTT
```

```
------------------------------------------------------------------
-------------------------rs211-3                        Static
  172.16.213.93               test1.example.com            /
                            1
------------------------------------------------------------------
-------------------------
   Next-Hop SLB Server       IP Type       Probe Dest IP
Address            Domain-Name                      URL
     Average RTT
------------------------------------------------------------------
-------------------------rs211                          Static
  172.16.213.93               test1.example.com            /
                            13
ACOS(config)# show slb link-probe entry server rs211
------------------------------------------------------------------
-------------------------
   Next-Hop SLB Server      IP Type
 Probe Dest IP Address           Domain-Name
 URL             Average RTT
------------------------------------------------------------------
-------------------------
       rs211                      Static    172.16.213.93
       test1.example.com                          /
                       10

ACOS(config)# show slb link-probe entry server rs211 detail

Next-Hop SLB Server      :     rs211
Probe Template Name   :     a
Domain-Name                 :      test1.example.com
URL                                  :      /

IP Type                              :      Static

Probe Dest IP Address    :     172.16.213.93
Current Probe in Test    :       1
Probes Per Test               :        10
Probe Interval (Seconds) :     2
Test Interval (Seconds)  :       1
```

```
RTT Method                        :       HTTP Req - Resp Latency
Last HTTP Status Code  :       200
Average RTT                :             11

RTT Individual Samples   :
-------------------------------------------------------------------
-------------------------
Sample#     | #1     | #2     | #3     | #4     | #5     | #6     |
#7     | #8     | #9     | #10    |
-------------------------------------------------------------------
-------------------------
ms          | 15     | 9      | 15     | 13     | 9      | 10     | 12
    | 13     | 12     | 11     |

ACOS(config)# show slb link-probe entry service-group sg1
-------------------------------------------------------------------
-------------------------
   Next-Hop SLB Server      IP Type      Probe Dest IP Address
          Domain-Name                   URL
Average RTT
-------------------------------------------------------------------
-------------------------
rs212                       Static    172.16.213.93
  test1.example.com          /                              33
-------------------------------------------------------------------
-------------------------
   Next-Hop SLB Server      IP Type      Probe Dest IP Address
          Domain-Name                   URL
Average RTT
-------------------------------------------------------------------
-------------------------
rs211-3                     Static    172.16.213.93
  test1.example.com          /                               1

-------------------------------------------------------------------
-------------------------
   Next-Hop SLB Server      IP Type      Probe Dest IP Address
          Domain-Name                   URL
Average RTT
```

```
-------------------------------------------------------------
-------------------------
rs211                        Static    172.16.213.93
  test1.example.com           /                              13

ACOS(config)# show slb link-probe entry service-group sg1
detail
Next-Hop SLB Server           :               rs212

Probe Template Name        :               a

Domain-Name                       :
test1.example.com
URL                                        :                /

IP Type                                   :
Static
Probe Dest IP Address        :                172.16.213.93

Current Probe in Test         :                 10

Probes Per Test                     :                10

Probe Interval (Seconds)    :                  2

Test Interval (Seconds)       :                  1

RTT Method                           :                HTTP Req
- Resp Latency
Last HTTP Status Code        :                  200

Average RTT                           :                   32

RTT Individual Samples       :
-------------------------------------------------------------
-------------------------
Sample#    | #1    | #2    | #3    | #4    | #5    | #6    |
#7    | #8    | #9    | #10   |
```

```
------------------------------------------------------------
-------------------------
ms          | 35     | 35     | 33     | 33     | 32     | 32     | 30
    | 36     | 36     | 27     |
```

The following command displays slb link probe statistics commands:

```
ACOS(config)# show slb link-probe statistics
Counter Name
------------------------------------------------------------
---
Total TCP Conn Sent                              0
Total HTTP Probes Sent                           0
Total HTTP responses rcvd                        0
Total HTTP expected status code rcvd             0
Total HTTP bad status code rcvd                  0
Total TCP Errors in Probe connections            0
Smart NAT Alloc Failures                         0
Smart NAT Port Alloc Failures                    0
L4 Session Alloc Failures                        0
TCP Connection Start Failed                      0
```

show slb mlb

Description Display statistics for message based load balancing (MBLB).

Syntax

```
show slb mlb [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command displays MBLB statistics:

```
ACOS# show slb mlb
                                                  Total
------------------------------------------------------------
----
Client message sent                              0
Server message received                          0
```

```
Server connection created                    0
Server connection rst                        0
Server connection failed                     0
Server connection closed                     0
Client connection created                    0
Client connection closed                     0
Client connection not found                  0
ACOS#
```

show slb mssql

Description Display statistics for database load-balancing (DBLB) for a MS-SQL database system.

Syntax

```
show slb mssql [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command displays MS-SQL statistics:

```
ACOS(config)# show slb mssql
                          Total
-------------------------------------------------------------
----
Curr Proxy Conns          0
Total Proxy Conns         0
Curr BE Encryption Conns  0
Total BE Encryption Conns 0
Curr FE Encryption Conns  0
Total FE Encryption Conns 0
Client FIN                0
Server FIN                0
Session err               0
DB Queries                0
DB commands reply         0
Authentication Success    0
Authentication Failure    0
```

The following table describes the fields in the command output.

Field	Description
Current Proxy Connections	Number of currently active connections that use the DBLB proxy.
Total Proxy Connections	Total number of connections that have used the DBLB proxy.
Current BE Encryption Connections	Number of currently active, encrypted connections on the back-end (BE), between the ACOS device and server which process database queries.
Total BE Encryption Connections	Total number of encrypted connections on the back-end (BE), between the ACOS device and server which process database queries.
Current FE Encryption Connections	Number of currently active, encrypted connections on the front-end (FE), between the ACOS device and a client.
Total FE Encryption Connections	Total number of encrypted connections on the front-end (FE), between the ACOS device and a client.
Client FIN	Number of TCP connections that were closed on the client side.
Server FIN	Number of TCP connections that were closed on the server side.
Session Error	Total number of session errors that occurred while processing DBLB requests.
DB Queries	Total number of received database queries. **NOTE:** This counter corresponds to the number of instances that the aFleX DB_QUERY event was triggered.
DB Commands Reply	Total number of received database commands.

Field	Description
	NOTE: This counter corresponds to the number of instances that the aFleX DB_COMMAND event was triggered.
Authentication Success	Number of successful AUTH commands.
Authentication Failure	Number of failed AUTH commands.

show slb mqtt

Description Shows SLB MQTT statistics.

Syntax

```
show slb mqtt
```

Parameter	Description
`detail`	Displays per DP statistics in the output.
`<vip> <vport>`	Displays port-specific MQTT statistics.

Mode All

Example The following command displays MQTT statistics:

```
ACOS# show slb mqtt
                                                    Total
-------------------------------------------------------------------
----
MQTT Connect                                          0
MQTT Connack                                          0
MQTT Publish                                          0
MQTT Puback                                           0
MQTT Pubrec                                           0
MQTT Pubrel                                           0
MQTT Pubcomp                                          0
MQTT Subscribe                                        0
MQTT Suback                                           0
MQTT Unsubscribe                                      0
MQTT Unsuback                                         0
MQTT Pingreq                                          0
MQTT Pingresp                                         0
MQTT Disconnect                                       0
MQTT Auth                                             0
MQTT Unknown                                          0
Current proxy conns                                   0
Total proxy conns                                     0
Total MQTT Commands                                   0
ACOS#
```

The following table describes the fields or MQTT packets shown in the output.

Field	Description
MQTT Connect	Client to Server connection request.
MQTT Connack	Server to Client connection acknowledgment.
MQTT Publish	Client to Server or Server to Client publish message.
MQTT Puback	Client to Server or Server to Client publish acknowledgment.
MQTT Pubrec	Client to Server or Server to Client publish

Field	Description
	received.
MQTT Pubrel	Client to Server or Server to Client publish release.
MQTT Pubcomp	Client to Server or Server to Client publish complete.
MQTT Subscribe	Client to Server subscribe request.
MQTT Suback	Server to Client subscribe acknowledgment.
MQTT Unsub-scribe	Client to Server unsubscribe request.
MQTT Unsuback	Server to Client unsubscribe acknow-ledgment.
MQTT Pingreq	Client to Server PING request.
MQTT Pingresp	Server to Client PING response.
MQTT Dis-connect	Client to Server or Server to Client disconnect notification.
MQTT Auth	Client to Server or Server to Client authen-tication exchange.
MQTT Unknown	Unknown requests or responses.
Current proxy conns	Current proxy connections.
Total proxy conns	Total proxy connections.
Total MQTT Com-mands	Total MQTT commands.

show slb mysql

Description Display statistics for database load-balancing (DBLB) for a MySQL database system.

Syntax

```
show slb mysql [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command displays MySQL statistics:

```
ACOS(config)# show slb mysql
                            Total
-------------------------------------------------------------------
----
Curr Proxy Conns            0
Total Proxy Conns           0
Curr BE Encryption Conns    0
Total BE Encryption Conns   0
Curr FE Encryption Conns    0
Total FE Encryption Conns   0
Client FIN                  0
Server FIN                  0
Session err                 0
DB Queries                  0
DB commands reply           0
```

The following table describes the fields in the command output.

Field	Description
Current Proxy Connections	Number of currently active connections that use the DBLB proxy.
Total Proxy Connections	Total number of connections that have used the DBLB proxy.
Current BE Encryption Connections	Number of currently active, encrypted connections on the back-end (BE), between the ACOS device and server which process database queries.
Total BE Encryption Connections	Total number of encrypted connections on the back-end (BE), between the ACOS device and server which process database queries.
Current FE	Number of currently active, encrypted connections

Field	Description
Encryption Connections	on the front-end (FE), between the ACOS device and a client.
Total FE Encryption Connections	Total number of encrypted connections on the front-end (FE), between the ACOS device and a client.
Client FIN	Number of TCP connections that were closed on the client side.
Server FIN	Number of TCP connections that were closed on the server side.
Session Error	Total number of session errors that occurred while processing DBLB requests.
DB Queries	Total number of received database queries. **NOTE:** This counter corresponds to the number of instances that the aFleX DB_QUERY event was triggered.
DB Commands Reply	Total number of received database commands. **NOTE:** This counter corresponds to the number of instances that the aFleX DB_COMMAND event was triggered.

show slb passthrough

Description Display statistics for pass-through TCP sessions. A pass-through TCP session is one that is not terminated by the ACOS device (for example, a session for which the ACOS device is not serving as a proxy for SLB).

Syntax

```
show slb passthrough
```

Mode All

Example The following command displays TCP pass-through session statistics:

```
ACOS# show slb passthrough
Request packets:      10741     Response packets:      38195
```

```
Request bytes:       570272     Response bytes:     56562872
Current connections:        0     Total connections:
4
```

show slb persist

Description Show persistence load-balancing statistics.

Syntax

```
show slb per [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Example The following command shows summary persistence statistics:

```
ACOS# show slb per
                          Total
-------------------------------------------------------------
----
URL hash persist(pri)     0
URL hash persist(sec)     0
URL hash persist fail     0
SRC IP persist ok         0
SRC IP persist fail       0
SRC IP hash persist(pri)  0
SRC IP hash persist(sec)  0
SRC IP hash persist fail  0
DST IP persist ok         0
DST IP persist fail       0
DST IP hash persist(pri)  0
DST IP hash persist(sec)  0
DST IP hash persist fail  0
SSL SID persist ok        0
SSL SID persist fail      0
Cookie persist ok         0
Cookie persist fail       0
Persist cookie not found  0
Persist cookie Pass-thru  0
Enforce higher priority   30
```

The following table describes the fields in the command output.

Field	Description
URL hash persist (pri)	Number of requests successfully sent to the primary server selected by URL hashing. The primary server is the one that was initially selected and then re-used based on the hash value.
URL hash persist (sec)	Number of requests that were sent to another server (a secondary server) because the primary server selected by URL hashing was unavailable.
URL hash persist fail	Number of requests that could not be fulfilled using URL hashing.
SRC IP persist ok	Number of requests successfully sent to the same server as previous requests from the same client, based on source-IP persistence.
SRC IP persist fail	Number of requests that could not be fulfilled by the same server as previous requests from the same client, based on source-IP persistence.
SRC IP hash persist (pri)	Number of requests successfully sent to the primary server selected by source IP hashing. The primary server is the one that was initially selected and then re-used based on the hash value.
SRC IP hash persist (sec)	Number of requests that were sent to another server (a secondary server) because the primary server selected by source IP hashing was unavailable.
SRC IP hash persist fail	Number of requests that could not be fulfilled using source IP hashing.
DST IP persist	Number of requests that were sent to the same resource, based on destination-IP persistence.

Field	Description
ok	
DST IP persist fail	Number of requests that could not be sent to the same resource, based on destination-IP persistence.
DST IP hash persist (pri)	Number of requests successfully sent to the primary server selected by destination IP hashing. The primary server is the one that was initially selected and then re-used based on the hash value.
DST IP hash persist (sec)	Number of requests that were sent to another server (a secondary server) because the primary server selected by destination IP hashing was unavailable.
DST IP hash persist fail	Number of requests that could not be fulfilled using destination IP hashing.
SSL SID persist ok	Number of requests successfully sent to the same server as previous requests that had the same SSL session ID, based on SSL session-ID persistence.
SSL SID persist fail	Number of requests that could not be fulfilled by the same server as previous requests that had the same SSL session ID, based on SSL session-ID persistence.
Cookie persist ok	Number of requests successfully sent to the same server as previous requests based on a persistence cookie.
Cookie persist fail	Number of requests that could not be fulfilled by the same server as previous requests based on a persistence cookie.
Persist cookie not found	Number of requests in which a persistence cookie was not found in the request header.

Field	Description
Persist cookie Pass-thru	Number of requests that contained a pass-through cookie.
Enforce higher priority	Number of times the enforce-higher-priority option overrode server persistence and selected another server.

show slb player-id-check-status

Description Displays the status of Player ID check enforcement.

Syntax

```
show slb player-id-check-status
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb player-id-check-status
state : Disabled
time_to_active : 0
table_count : 0
```

Field	Description
state	Indicates whether the Player ID check feature is currently enabled or disabled.
time_to_active	Shows the time remaining for the Player ID check to become active, measured in seconds.
table_count	Displays the number of entries in the Player ID check table.

show slb player-id-records-all

Description Displays Layer 7 (L7) session statistics for each data plane.

Syntax `show slb player-id-records-all`

Mode All

Usage Used for monitoring and troubleshooting player-related information.

Example The following example displays sample output:

```
ACOS# show slb player-id-records-all
```

show slb player-id-stats

Description Displays Layer 7 (L7) session statistics for each data plane.

Syntax `show slb player-id-stats`

Mode All

Example The following example displays sample output:

```
ACOS# show slb player-id-stats
-------------------------------------------------------
Counter                                          Value
-------------------------------------------------------
Playerid records created                             0
Playerid records deleted                             0
Playerid records max time aged out                   0
Playerid records idle timeout                        0
Invalid playerid packets                             0
Invalid playerid packet drops                        0
Valid playerid packets                               0
```

Field	Description
`Playerid records created`	Number of player ID records created.
`Playerid records deleted`	Number of player ID records deleted.
`Playerid records max time aged out`	Number of player ID records that have aged out due to maximum

Field	Description
	time.
Playerid records idle timeout	Number of player ID records that have timed out due to inactivity.
Invalid playerid packets	Number of packets with invalid player IDs.
Invalid playerid packet drops	Number of packets with invalid player IDs that were dropped.
Valid playerid packets	Number of packets with valid player IDs.

show slb pop3-proxy

Description Show POP3 proxy statistics

Syntax

```
show slb pop3-proxy [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example Example output for this command:

```
ACOS-Inside# show slb pop3-proxy
                            Total
-------------------------------------------------------------
----
Current proxy conns         0
Total proxy conns           0
Total POP3 Request          0
Server selection failure    0
no route failure            0
source nat failure          0
request line freed          0
request line freed          0
invalid start line          0
```

```
other cmd                   0
line too long               0
Control chn ssl             0
Bad Sequence                0
Serv Sel Persist fail       0
Serv Sel SMPv6 fail         0
Serv Sel SMPv4 fail         0
Serv Sel ins tpl fail       0
Client EST state erro       0
Serv CTNG state erro        0
Serv RESP state erro        0
Client RQ state erro        0
```

show slb quic

Description Shows the SLB QUIC statistics.

Syntax

```
show slb quic
```

Mode All

Example The following command shows the SLB QUIC statistics.

```
ACOS# show slb quic
```

	Total
Client connection attempted	1
Client connection handshake	1
Client connection created	1
Client connection local closed	1
Client connection remote closed	0
Client connection failed	0
Server connection attempted	1
Server connection handshake	1
Server connection created	1
Server connection local closed	1
Server connection remote closed	0
Server connection failed	0
QUIC conn created	2
QUIC conn freed	2
Local bi-stream created	1
Remote bi-stream created	1
Local bi-stream closed	2
Remote bi-stream closed	6
Local uni-stream created	6
Remote uni-stream created	7
Local uni-stream closed	0
Remote uni-stream closed	0
Stream error	0
Padding frame receive	4
Padding frame send	25
Ping frame receive	4
Ping frame send	0
Ack frame receive	9
Ack frame send	14
Ack ECN frame receive	0
Ack ECN frame send	0
Stream reset frame receive	0
Stream reset frame send	6
Stream stop frame receive	0
Stream stop frame send	0
Crypto frame receive	7

Crypto frame send	9
New token frame receive	0
New token frame send	1
Stream frame receive	0
Stream frame send	0
Stream_09 frame receive	0
Stream_09 frame send	0
Stream_0a frame receive	3
Stream_0a frame send	7
Stream_0b frame receive	1
Stream_0b frame send	1
Stream_0c frame receive	0
Stream_0c frame send	0
Stream_0d frame receive	0
Stream_0d frame send	0
Stream_0e frame receive	5
Stream_0e frame send	1
Stream_0f frame receive	2
Stream_0f frame send	1
Max data frame receive	0
Max data frame send	0
Max stream data frame receive	0
Max stream data frame send	1
Max bi-stream frame receive	0
Max bi-stream frame send	0
Max uni-stream frame receive	0
Max uni-stream frame send	0
Data blocked frame receive	0
Data blocked frame send	0
Stream data blocked frame receive	0
Stream data blocked frame send	0
Bi-stream data blocked frame receive	0
Bi-stream data blocked frame send	0
Uni-stream data blocked frame receive	0
Uni-stream data blocked frame send	0
New conn id frame receive	0
New conn id frame send	1
Retire conn id frame receive	0

Retire conn id frame send	0
Path challenge frame receive	0
Path challenge frame send	0
Path response frame receive	0
Path response frame send	0
Conn close frame receive	0
Conn close frame send	0
App conn close frame receive	0
App conn close frame send	0
Handshake done frame receive	0
Handshake done frame send	0
Unknown frame	0
Stream FIN receive	0
Stream FIN up	0
Stream FIN down	0
Stream FIN send	0
Stream congest	0
Stream open	0
Stream pause data	0
Stream resume data	0
Stream not send	0
Stream created	0
Stream freed	0
Initial receive	0
Initial send	0
RTT_0 receive	0
RTT_0 send	0
Handshake receive	0
Handshake send	0
Retry receive	0
Retry send	0
Version negotiation receive	0
Version negotiation send	0
RTT updated	0
Needs ACK	0
ACK rescheduled	0
Packet receive	0
Packet send	0

Packet send failed	0
Congestion window increase	0
Congestion window decrease	0
No congestion window	0
Burst limited	0
Packet loop limited	0
Receive window limited	0
Parse error	0
Conn closed of error	0
Unknown SCID	0
DCID mismatch	0
Packet too short	0
Invalid version	0
Invalid packet	0
Invalid conn match	0
Invalid session packet	0
Stateless reset	0
Packet lost	0
Packet drop	0
Packet retransmit	0
Packet out of order	0
Quic packet drop	0
Encode error	0
Decode failed	0
Decode stream error	0
Exceed_flow_control	0
Tx buffer enqueued	0
Tx buffer dequeued	0
App buffer enqueued	0
App buffer dequeued	0
App buffer queue full	0
Iov buffer bind	0
Iov buffer unbind	0
Iov buffer dup	0
Iov alloc len	0
No tx queue	0
Wsocket created	0
Wsocket closed	0

```
A10 socket created                          0
A10 socket closed                           0
No A10 socket                               0
No other side socket                        0
Lost detection timeout                      0
Connection idle timeout                     0
ACK timeout                                 0
QUIC malloc                                 0
QUIC free                                   0
QUIC malloc failure                         0
QUIC malloc failure                         0
QUIC LB                                     0
CID Zero                                    0
Invalid CID Signature                       0
QUIC TLS key update received                0
QUIC TLS key update sent                    0
```

The following table describes the fields in the command output.

Counters	Description
Client connection attempted	Displays the client-side QUIC connection-specific statistics.
Client connection handshake	
Client connection created	
Client connection local closed	
Client connection remote closed	

Counters	Description
Client connection failed	
Server connection attempted	Displays the server-side QUIC connection-specific statistics.
Server connection handshake	
Server connection created	
Server connection local closed	
Server connection remote closed	
Server connection failed	
QUIC conn created	Displays the number of QUIC connection created and freed.
QUIC conn freed	
Local bi-stream created	Displays the number of local and remote bidirectional stream created or closed.
Remote bi-stream created	
Local bi-stream	

Counters	Description
closed	
Remote bi-stream closed	
Local uni-stream created	Displays the number of local and remote uni-directional stream created or closed.
Remote uni-stream created	
Local uni-stream closed	
Remote uni-stream closed	
Stream error	Displays the number of errors occurred and reset in the stream.
Padding frame receive	Displays the number of PADDING frames sent and received. PADDING frame (type=0x00) is used to expand a packet size.
Padding frame send	
Ping frame receive	Displays the number of PING frames sent and received. PING frame (type=0x01) is used to check whether their endpoints are still alive or reachable.
Ping frame send	
Ack frame receive	Displays the number of ACK frames sent and received. ACK frame (types 0x02 and 0x03) is used to notify to the senders of received and processed packets.
Ack frame send	

Counters	Description
Ack ECN frame receive	Displays the number of ACK Explicit Congestion Notification (ECN) frames sent and received. The ACK frame indicates ECN feedback and reports receipt of QUIC packets with associated ECN codepoints.
Ack ECN frame send	
Stream reset frame receive	Displays the number of RESET_STREAM frames sent and received. RESET_STREAM frame (type=0x04) is used to terminate the sent portion of a stream abruptly.
Stream reset frame send	
Stream stop frame receive	Displays the number of STOP_STREAM frames sent and received. STOP_STREAM frame (type=0x05) is used to indicate that incoming data will be discarded upon receipt of the application request.
Stream stop frame send	
Crypto frame receive	Displays the number of CRYPTO frames sent and received. CRYPTO frame (type=0x06) is used to transmit the cryptographic handshake messages.
Crypto frame send	
New token frame receive	Displays the number of new tokens sent and received by the server from a client to establish a new connection.
New token frame send	
Stream frame receive	Displays the number of STREAM frames sent and received. STREAM frame is used to create and transport streams. The STREAM frame has the format 0b00001XXX (or the set of values from 0x08 to 0x0f).
Stream frame send	
Stream_09 frame receive	
Stream_09 frame send	

Counters	Description
Stream_0a frame receive	
Stream_0a frame send	
Stream_0b frame receive	
Stream_0b frame send	
Stream_0c frame receive	
Stream_0c frame send	
Stream_0d frame receive	
Stream_0d frame send	
Stream_0e frame receive	
Stream_0e frame send	
Stream_0f frame receive	
Stream_0f frame send	
Max data frame receive	Displays the number of MAX_DATA frames sent and received. MAX_DATA frame (type=0x10) is used in flow control to inform a endpoint of the maximum amount of data that can be sent in the connection.
Max data frame send	
Max stream data frame	Displays the number of MAX_STREAM_DATA frames sent and received.

Counters	Description
receive	MAX_STREAM_DATA frame (type=0x11) is used in flow control to inform a peer of the maximum amount of data that can be sent on a stream.
Max stream data frame send	
Max bi-stream frame receive	Displays the number of MAX_STREAMS bidirectional frames sent and received. MAX_STREAMS frame with a type of 0x12 applies to bidirectional streams.
Max bi-stream frame send	
Max uni-stream frame receive	Displays the number of MAX_ STREAMS unidirectional frames sent and received. MAX_STREAMS frame with a type of 0x13 applies to unidirectional streams.
Max uni-stream frame send	
Data blocked frame receive	Displays the number of DATA_BLOCKED frames sent and received. DATA_BLOCKED frame (type=0x14) is used when it wishes to send data but is unable to do so due to connection-level flow control.
Data blocked frame send	
Stream data blocked frame receive	Displays the number of STREAM_DATA_ BLOCKED frames sent and received. STREAM_DATA_BLOCKED frame (type=0x15) is used when it wishes to send data but is unable to due to stream-level flow control.
Stream data blocked frame send	
Bi-stream data blocked frame receive	Displays the number of STREAM_ BLOCKED bidirectional frames sent and received. STREAMS_BLOCKED frame of type 0x16 is used to indicate that the bidirectional stream limit has been

Counters	Description
Bi-stream data blocked frame send	reached.
Uni-stream data blocked frame receive	Displays the number of STREAM_ BLOCKED unidirectional frames sent and received. STREAMS_BLOCKED frame of type 0x17 is used to indicate that the unidirectional stream limit has been reached.
Uni-stream data blocked frame send	
New conn id frame receive	Displays the number of NEW_CONNECTION_ ID frames sent and received. NEW_CONNECTION_ID frame (type=0x18) is used to provide its endpoints with alternative connection IDs, which can be used to break the links when migrating connections.
New conn id framesend	
Retire conn id frame receive	Displays the number of RETIRE_CONNECTION_ ID frames sent and received. RETIRE_CONNECTION_ID frame (type=0x19) is used to indicate that a connection ID issued by its endpoints can no longer be used.
Retire conn id frame send	
Path chal-lenge frame receive	Displays the number of PATH_CHALLENGE frames sent and received. PATH_CHALLENGE frame (type=0x1a) is used to validate paths and check reachability to the endpoints during connection migration.
Path chal-lenge frame send	
Path response frame receive	Displays the number of PATH_RESPONSE frames sent and received. PATH_RESPONSE frame (type=0x1b) is sent in response to a PATH_CHALLENGE frame.
Path response	

Counters	Description
frame send	
Conn close frame receive	Displays the number of CONNECTION_CLOSE frames sent and received. CONNECTION_CLOSE frames (type=0x1c or 0x1d) are used to notify to an endpoint that the connection is being closed.
Conn close frame send	
App conn close frame receive	Displays the number of application-specific CONNECTION_CLOSE frames sent and received. If an application wishes to abandon a connection during the handshake, an endpoint can send a CONNECTION_CLOSE frame (type 0x1c) with an error code in an Initial or Handshake packet.
App conn close frame send	
Handshake done frame receive	Displays the number of HANDSHAKE_DONE frames sent and received. HANDSHAKE_DONE frame (type=0x1e) is used to signal the client that the handshake has been completed.
Handshake done frame send	
Unknown frame	Displays the number of FRAME_ENCODING_ERROR errors occured. FRAME_ENCODING_ERROR frame is used to notify to the endpoints that the frame was improperly formatted or is of an unknown type.
Stream FIN receive	Displays the number of FIN messages received, sent, up, and down in the STREAM data. The application indicates that all stream data has been sent, along with a STREAM frame containing the FIN bit. The sent portion of the stream enters the "Data Sent" state.
Stream FIN up	
Stream FIN down	
Stream FIN send	

Counters	Description
Stream congest	Displays the STREAM frames-related statistics.
Stream open	
Stream pause data	
Stream resume data	
Stream not send	
Stream created	
Stream freed	
Initial receive	Displays the number of Initial packets sent and received. Initial packet uses long headers with a value of 0x0. It transports the first CRYPTO frames sent by the client and server to exchange keys and ACKs in either direction.
Initial send	
RTT_0 receive	Displays the number of RTT_0 packets sent and received. 0-RTT packet uses long headers with a value of 0x1, followed by the Length and Packet Number fields.
RTT_0 send	
Handshake receive	Displays the number of Handshake packets sent and received. Handshake packet uses long headers with a value of 0x2, followed by the Length and Packet Number fields.
Handshake send	

Counters	Description
Retry receive	Displays the number of Retry packets sent and received. Retry packet uses a long packet header with a value of 0x3. It contains a server-generated address validation token.
Retry send	
Version negotiation receive 0	Displays the number of Version negotiation packets sent and received. The Version Negotiation packet is not version-specific. When a client receives it, it is identified as a Version Negotiation packet because the Version field has a value of 0.
Version negotiation send	
RTT updated	Displays the number of 1-RTT packets updated. The 1-RTT packet or handshake indicates that the client side handshake is complete.
Needs ACK	Displays the number of packets that needs ACK.
ACK rescheduled	Displays the number of packets rescheduled for ACK.
Packet receive	Displays the number of packets received, sent, and failed.
Packet send	
Packet send failed	
Congestion window increase	Displays the number of congestion window increased and decreased. Congestion Window is a QUIC state variable that controls how much data QUIC can send over the network before receiving an ACK.
Congestion window decrease	
No congestion win-	

Counters	Description
dow	
Burst limited	Displays the number of bursts that were limited while the initial congestion window is displayed.
Packet loop limited	Displays the number of packet loops that were limited while the initial congestion window is displayed.
Receive window limited	Displays the number of receive window that were limited.
Parse error	Displays the number of errors that were parsed.
Conn closed of error	Displays the number of errors occurred while closing the connection.
Unknown SCID	Displays the number of unknown source connection ID (SCID).
DCID mismatch	Displays the number of destination connection ID (DCID) that were mismatched.
Packet too short	Displays the number of packets that were too short.
Invalid version	Displays the number of packet versions that were invalid.
Invalid packet	Displays the number of packets that were invalid.
Invalid conn match	Displays the number of invalid connections that were matched.
Invalid session packet	Displays the number of session packets that were invalid.
Stateless reset	Displays the number of stateless reset tokens that were used.

Counters	Description
Packet lost	Displays the packet-related statistics.
Packet drop	
Packet retransmit	
Packet out of order	
Quic packet drop	
Encode error	Displays the number of encode errors occurred in QUIC connection.
Decode failed	Displays the number of decode failed in QUIC connection.
Decode stream error	Displays the number of decode errors occurred in the STREAM.
Exceed_flow_control	Displays the number of flow control limits exceeded.
Tx buffer enqueued	Displays the number of transmission (tx) buffers that were enqueued or dequeued.
Tx buffer dequeued	
App buffer enqueued	Displays the number of application transmission (tx) buffers that were enqueued, dequeued, or full.
App buffer dequeued	
App buffer queue full	
Iov buffer bind	
Iov buffer unbind	

Counters	Description
Iov buffer dup	
Iov alloc len	
No tx queue	
Wsocket created	Displays the number of web sockets that were closed and created.
Wsocket closed	
A10 socket created	Displays the A10 socket-related statistics.
A10 socket closed	
No A10 socket	
No other side socket	
Lost detection timeout	Displays the number of loss detection that were timed out.
Connection idle timeout	Displays the number of connections that were timed out because of set idle timeout.
ACK timeout	Displays the number of ACK packets that were timed out.
QUIC malloc	Displays the number of memories allocated, freed, and failed for QUIC processing.
QUIC free	
QUIC malloc failure	
QUIC LB	Displays the number of QUIC connections that were load balanced.
CID Zero	Displays the number of connection IDs that had zero value.

Counters	Description
Invalid CID Signature	Displays the number of connection IDs that had invalid signature.
QUIC TLS key update received	Displays the number of times the key updates were received and sent during the QUIC-TLS handshake.
QUIC TLS key update sent	

show slb rate-limit-for-reset-unknown-conn

Description Displays rate limiting of reset packets for unknown connection.

Syntax

```
show slb rate-limit-for-reset-unknown-conn
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb rate-limit-for-reset-unknown-conn
Rate limit for unknown-reset-conn:
-------------------------------------
Rate limit:
Current rate:
Rate limit drops:
```

Field	Description
`Rate limit`	The rate limit for reset packets for unknown connections.
`Current rate`	Current rate of reset packets received for unknown connections.
`Rate limit drops`	Number of reset packets dropped due to rate limit being exceeded.

show slb rate-limit-logging

Description Show log rate-limiting statistics.

Syntax

```
show slb rate-limit-logging [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows log rate-limiting statistics:

```
ACOS# show slb rate-limit-logging
Total
-----------------------------------------------------------------
----
Total log times           51
Total log messages        26
Local log messages        190
Remote log messages       1959
Local rate (per sec)      32
Remote rate (per sec)     453
Log message too big       0
No route                  0
Buffer alloc fail         0
Buffer send fail          0
Log-session alloc         15
Log-session free          15
Log-session alloc fail    0
No repeat message         4
```

The following table describes the fields in the command output.

Field	Description
Total log times	Total number of times log rate limiting has been used.
Total log	Total number of log messages generated by the ACOS

Field	Description
messages	device. **NOTE:** The ACOS device combines repeated messages into a single message. For this reason, the Total log times count will differ from the Total log messages count.
Local log messages	Total number of log messages in the ACOS device's log buffer. These messages can be displayed using the **`show log`** command.
Remote log messages	Total number of log messages the ACOS device has sent to external log servers.
Local rate (per sec)	Number of messages sent to the ACOS device's log buffer during the most recent one-second interval.
Remote rate (per sec)	Number of messages sent to external log servers during the most recent one-second interval.
Log message too big	Number of log messages dropped by the ACOS device because they were too long.
No route	Number of log messages dropped by the ACOS device because the device did not have a route to the log server.
Buffer alloc fail	Number of times the ACOS device was unable to allocate a buffer for sending a log message to an external log server.
Buffer send fail	Number of times the ACOS device was unable to send a log message that had been placed in the buffer for sending to an external log server.
Log-session alloc	Number of times the ACOS device allocated a log session for repeated log messages.

Field	Description
Log-session free	Number of times the ACOS device freed a log session that was allocated for repeated log messages.
Log-session alloc fail	Number of times the ACOS device was unable to allocate a log session for repeated log messages.
No repeat message	Number of times there was no repeated message for a log session allocated for repeated messages.

show slb resource-usage

Description Display the minimum and maximum numbers of SLB resources that can be configured or used, the default maximum number allowed by the configuration, and the number currently in use are platform specific.

Syntax

```
show slb resource-usage
```

Example Below is an example of the output for this command:

```
ACOS# show slb resource-usage

Resource                          Current    Default    Minimum
   Maximum
------------------------------------------------------------------
------------
nat-pool-addr-count               10         10         10
   2000
real-server-count                 128        128        32
   8192
real-port-count                   256        256        64
   16384
service-group-count               128        128        32
   8192
virtual-port-count                128        128        32
   8192
virtual-server-count              64         64         16
   4096
```

cache-template-count	128	128	32
2048			
http-template-count	128	128	32
4096			
fix-template-count	128	128	32
4096			
link-cost-template-count	16	16	16
16			
log-template-count	128	128	32
4096			
pbslb-entry-count	100000	100000	100000
1000000			
proxy-template-count	128	128	32
4096			
conn-reuse-template-count	128	128	32
4096			
fast-tcp-template-count	128	128	32
4096			
fast-udp-template-count	128	128	32
4096			
client-ssl-template-count	128	128	32
8192			
server-ssl-template-count	128	128	32
8192			
stream-template-count	128	128	32
4096			
persist-cookie-template-count	128	128	32
4096			
persist-srcip-template-count	128	128	32
4096			
health-monitor-count	1023	1023	512
1024			
pbslb-subnet-count	65536	65536	65536
65536			
gslb-site-count	500	500	500
500			
gslb-device-count	1000	1000	1000
1000			

```
gslb-service-ip-count              128         128         32
   5000
gslb-service-port-count            256         256         64
   10000
gslb-zone-count                    5000        5000        5000
   5000
gslb-service-count                 10000       10000       10000
   10000
gslb-policy-count                  10000       10000       10000
   10000
gslb-geo-location-count            5000000     5000000     5000000
   5000000
gslb-ip-list-count                 500         500         500
   500
gslb-template-count                1000        1000        1000
   1000
gslb-svc-group-count               500         500         500
   500
slb-threshold-res-usage-percent    0           0           1
   99
```

show slb server

Description Show information about real servers.

Syntax

```
show slb server [bindings]
```

or

```
show slb server
[server-name [port-num]
   [all-partitions | partition {shared | name} | detail] |
[config]
   [all-partitions | partition {shared | name}] |
[connection-reuse]
   [all-partitions | partition {shared | name}] |
[auto-nat-stats]
   [all-partitions | partition {shared | name}]
[ip-nat-stats]
```

Parameter	Description
server-name	Shows information only for the specified server or

Parameter	Description
[[*port-num*] **detail**	port. If you omit this option, information is shown for all real servers and ports. IPv6 address support available. For example: DRS-2001:133::16-http1.example.com The **detail** option shows statistics for the specified server or port. This option also displays the name of the server or port template bound to the server or port with IPv4 or IPv6 address (for example: 2001:133::16).
bindings	Shows the bindings for real server ports.
config	Shows the SLB configuration of the real servers.
connection-reuse	Shows connection-reuse state information and statistics for the real servers.
auto-nat-stats	Shows statistics for Smart NAT.
ip-nat-stats	Shows statistics for IP NAT.
all-partitions	Show SLB server configuration for all partitions.
partition {shared | *name*}	Show SLB server configuration for either the shared partition, or the specified L3V partition *name*. Dynamic server name: Dynamic server IP address:

Mode All

Example The following command shows the output for the basic **show slb server** command. The “State”

```
ACOS# show slb server
Total Number of Servers configured: 1
Total Number of Services configured: 1
                    Current = Current Connections, Total =
Total Connections
```

```
                    Fwd-pkt = Forward packets, Rev-pkt =
Reverse packets
Service             Current   Total  Fwd-pkt  Rev-pkt  Peak-
conn  State
-----------------------------------------------------------------
--------
test-s1:80/tcp      0          0     0        0          0
Disb/Down
test-s1: Total      0          0     0        0          0
Disb/Down
```

Example The following command shows SLB statistics for real server “http1”. This server is in a service group that is bound to an HTTP virtual port:

```
ACOS# show slb server http1
Total Number of Services configured on Server http1: 1
Service: http1:80/tcp (Status: Up)
Forward packets:        0     Reverse packets:         0
Forward bytes:          0     Reverse bytes:           0
Current connections:    0     Persistent connections: 0
Current requests:       0     Total requests:          0
Total connections:      0     Total requests succ:     0
Response time:          0     tick
Peak connections:       0
Health-check:
-----------------------------------------------------------
Up reason:              HTTP Status Code OK
Monitor name:           http
Method:                 HTTP
Attribute:              port=80
                        url="GET /"
Wait for HTTP response:False
L4 conn made:           938
L4 errors:              0
Health-check average RTT (us):15930
Health-check current RTT (us):15958
Health-check average TCP RTT (us):7895
Health-check current TCP RTT (us):7933
HTTP requests sent:     938
HTTP errors:            0
Received OK:            938
```

```
Received error:         0
Response timeout:       0
```

Example

The following table describes out fields for the **`show slb server`** command. The output from this command includes statistics for health check fields. Keep in mind that these health check fields only appear in the output for HTTP traffic. The counters begin when the health check is configured and increment until the statistics are cleared or the health check is deleted.

Field	Description
Total Number of Services configured	Total number of services configured on the ACOS device (if a server name is not specified) or on the specified server.
Service	Real server name, service protocol port, and transport protocol (TCP or UDP), and Status (Up/Down/Disabled)
Forward packets	Number of request packets received for the service.
Reverse packets	Number of response packets sent on behalf of the real server.
Forward bytes	Number of request bytes received for the service.
Reverse bytes	Number of response bytes sent on behalf of the real server.
Current	Current number of connections to the service.
Persistent connections	Number of persistent connections to the service.
Current requests	Current number of requests to the service.
Total requests	Total number of requests to the service.
Total connections	Total number of connections to the service.

Field	Description
Total requests succ	Total number of requests to the service successfully received.
Response time	Server response time.
Peak-conn	Peak connection rate. **NOTE:** Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see extended-stats (individual server) or extended-stats (global).
Health check fields (HTTP traffic only)	
Up / Down reason	Reason the ACOS device marked the port up or down.
Monitor name	Name of the health monitor used to perform the health check.
Method	Health method in the monitor used for the health check.
Attribute	The destination TCP port of the health check, and the HTTP request sent to the port.
Wait for HTTP response	Indicates whether the ACOS device is still waiting for a response to the HTTP request.
L4 conn made	Total number of Layer 4 connections made to the destination TCP port for health checking.
L4 errors	Total number of Layer 4 errors that occurred during health checking.
Health-check average RTT	The average length of time it took for each health check. The time is expressed in microseconds (us). This counter includes the entire health-check process.
Health-check current RTT	The length of time it took to perform the most recent health check.

Field	Description
Health-check average TCP RTT	The average length of time it took to complete the 3-way handshake with the server port.
Health-check current TCP RTT	The length of time it took to complete the 3-way handshake in the most recent health check.
HTTP requests sent	Total number of HTTP requests sent to the server as part of health checks.
HTTP errors	Total number of HTTP errors that occurred during health checking.
Received OK	Number of times the payload of a Layer 4 health check reply was successfully read by the ACOS device.
Received error	Number of times a a read failure occurred in the a10hm module.
Response timeout	Number of times a health check to the port timed out.

NOTE: The same health check fields appear in the output for the show slb service-group *group-name* and similarly only apply to HTTP traffic.

Example The following command shows details for a real server with IPv4 address:

```
ACOS# show slb server dang0 detail
Server name:                                    dang0
Server IP address:                              192.168.120.21
Server gateway ARP:                             0000:0000:0000
State:                                          Down
Server template:                                default
   Health check:                                default
Current connection:                             0
Current request:                                0
Total connection:                               0
Total request:                                  0
Total request success:                          0
```

```
Total forward bytes:                              0
Total forward packets:                            0
Total reverse bytes:                              0
Total reverse packets:                            0
Peak connection:                                  0
```

The following command shows details for a real server with IPv6 address:

```
ACOS# show slb server http1 detail
Server name:                                      http1
Hostname:
http1.example.com
Last DNS reply:                                   Mon May 14
18:43:57 2018
Server gateway ARP:                               0000:0000:0000
State:                                            Up
Server template:                                  default
   Health check:                                  default
Current connection:                               0
Current request:                                  0
Total connection:                                 0
Total request:                                    0
Total request success:                            0
Total forward bytes:                              0
Total forward packets:                            0
Total reverse bytes:                              0
Total reverse packets:                            0
Peak connection:                                  0
Dynamic server name:                              DRS-
2001:133::16-http1.example.com
Dynamic server IP address:                        2001:133::16
Last DNS reply:                                   Mon May 14
18:43:57 2018
TTL:                                              86400
Server gateway ARP:                               000c:29fc:ee32
State:                                            Up
Server template:                                  default
   Health check:                                  default
Current connection:                               0
```

```
Current request:                                0
Total connection:                               0
Total request:                                  0
Total request success:                          0
Total forward bytes:                            0
Total forward packets:                          0
Total reverse bytes:                            0
Total reverse packets:                          0
Peak connection:                                0
Dynamic server name:                            DRS-
172.16.133.16-http1.example.com
Dynamic server IP address:                      172.16.133.16
Last DNS reply:                                 Mon May 14
18:43:56 2018
TTL:                                            86399
Server gateway ARP:                             000c:29fc:ee32
State:                                          Up
Server template:                                default
   Health check:                                default
Current connection:                             0
Current request:                                0
Total connection:                               0
Total request:                                  0
Total request success:                          0
Total forward bytes:                            0
Total forward packets:                          0
Total reverse bytes:                            0
Total reverse packets:                          0
Peak connection:                                0
```

The following table describes the fields in the command output.

Field	Description
Server name	Name of the server. IPv6 address support available. For example: DRS-2001:133::16-http1.example.com
Server IP address	IP address of the server. For the specified server or port. This option also displays the name of the server or port template bound to the server or port with

Field	Description
	IPv4 or IPv6 address (for example: 2001:133::16).
Server gateway ARP	Server ARP value (if directly connected) or nexthop ARP value (if connected through a gateway).
State	Current state of the service: • Up • Down • Disabled
Server template	Name of the real server template bound to the server.
Health check	Name of the health monitor used to check the health of the real port.
Current connection	Current number of connections to the port.
Current request	Current number of HTTP requests being processed by the port. **NOTE:** In this field and the Total request and Total request success fields, Layer 7 requests are counted only if Layer 7 request accounting is enabled using enable-l7-req-acct
Total connection	Total number of connections that have been made to the port.
Total request	Total number of HTTP requests processed by the port.
Total request success	Total number of HTTP requests that were successful.
Total forward bytes	Number of request bytes forwarded to the port.

Field	Description
Total forward packets	Number of request packets forwarded to the port.
Total reverse bytes	Number of request bytes received from the port.
Total reverse packets	Number of request packets received from the port.
Peak connection	Peak connection count. **NOTE:** Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see extended-stats (individual server) or extended-stats (global).

Example

The following command shows details for a real port on a server:

```
ACOS(config)# show slb server dang1 80 detail
Server name:                                    dang1
Port:                                           1.1.1.1:80
State:                                          Up
Port template:                                  default
   Health check:                                default
Current connection:                             53
Current request:                                42
Total connection:                               10011
Total request:                                  20090
Total request success:                          20089
Total forward bytes:                            36378463
Total forward packets:                          378463
Total reverse bytes:                            463784638
Total reverse packets:                          3784638
Peak connection:                                24411
```

The following table describes the fields in the command output.

Field	Description
Server name	Name of the server.
Server IP address	IP address of the server.
Server gateway ARP	Server ARP value (if directly connected) or nexthop ARP value (if connected through a gateway).
Port	Real port number.
State	Current state of the service: • Up • Down • Disabled
Port template	Name of the real port template bound to the port.
Health check	Name of the health monitor used to check the health of the real port.
Current connection	Current number of connections to the port.
Current request	Current number of HTTP requests being processed by the port. In this field and the Total request and Total request success fields, Layer 7 requests are counted only if Layer 7 request accounting is enabled using enable-l7-req-acct.
Total connection	Total number of connections that have been made to the port.
Total request	Total number of HTTP requests processed by the port.
Total request success	Total number of HTTP requests that were successful.

Field	Description
Total forward bytes	Number of request bytes forwarded to the port.
Total forward packets	Number of request packets forwarded to the port.
Total reverse bytes	Number of request bytes received from the port.
Total reverse packets	Number of request packets received from the port.
Peak connection	Peak connection count. **NOTE:** Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see extended-stats (individual server) or extended-stats (global).

Example

The following command displays detailed information for a dynamic hostname server. The configuration details are shown first, followed by details for the dynamically created servers.

```
ACOS# show slb server s-test1 detail
Server name:                              s-test1
Hostname:                                 s1.test.com
Last DNS reply:                           Tue Nov 17 03:41:59 2009
State:                          Up
Server template:                                    temp-server
   DNS query interval:                              5
   Minimum TTL ratio:                               3
   Maximum dynamic server:                          16
   Health check:                                    none
Current connection:                                 0
Current request:                                    0
Total connection:                                   1919
Total request:                             1919
```

```
Total request success:                          1877
Total forwarded byte:                           546650
Total forwarded packet:                         5715
Total received byte:                            919730
Total received packet:                          5631
Dynamic server name:            DRS-10.4.2.5-s1.test.com
Last DNS reply:                 Tue Nov 17 03:41:59 2009
TTL:                            4500
State:                          Up
Server template:                                test
   DNS query interval:                          5
   Minimum TTL ratio:                           15
   Maximum dynamic server:                      1023
   Health check:                                none
Current connection:                             0
Current request:                                0
Total connection:                               1919
Total request:                          1919
Total request success:                          1877
Total forward bytes:                            546650
Total forward packets:                          5715
Total reverse bytes:                            919730
Total reverse packets:                          5631
```

Example The following command shows SLB configuration information for real servers:

```
ACOS# show slb server config
Total Number of Services configured: 30
       H-check = Health check   Max conn = Max. Connection
Wgt = Weight
Service                Address         H-check  Status   Max
conn Wgt
-------------------------------------------------------------
-------
1_yahoo_finance:80/tcp 69.147.86.163   None     Enable
1000000  1
1_yahoo_finance        69.147.86.163   None     Enable
1000000  1
1_cybozu:80/tcp        202.218.147.129 None     Enable
1000000  1
```

```
1_cybozu                  202.218.147.129 None      Enable
1000000  1
win20:25/tcp              172.22.66.20    Default   Enable
1000000  1
win20                     172.22.66.20    ping      Disable
1000000  1
win21:25/tcp              172.22.66.21    Default   Enable
1000000  1
--MORE--
```

The following table describes the fields in the command output.

Field	Description
Total Number of Services configured	Total number of SLB services configured on the ACOS device.
Service	Real server name, service protocol port, and transport protocol (TCP or UDP).
Address	Real IP address of the server.
H-check	Health check enabled for the service: • None – No health check has been applied to the service. • Default – The default health monitor for the service type was automatically applied to the service by the ACOS device. • Name of a configured health monitor (for example, “ping”) – The named health monitor was applied to the service by an ACOS administrator.
Status	Current administrative status of the service: • Enable • Disable
Max conn	Maximum number of connections allowed to the service.
Wgt	Administrative weight assigned to the service.

Example The following command shows connection-reuse state information and statistics for real servers:

```
ACOS# show slb server connection-reuse
Total Number of Services configured: 30
Service                    State      Persistent-Conn
-------------------------------------------------------
1_yahoo_finance:80/tcp     Up         0

1_cybozu:80/tcp            Up         0

win20:25/tcp               Down       0

win21:25/tcp               Up         0
win21:110/tcp              Up         0
win21:80/tcp               Up         0
win21:443/tcp              Down       0

linux22:25/tcp             Disb       0
linux22:80/tcp             Up         0
linux22:53/udp             Disb       0
```

The following table describes the fields in the command output.

Field	Description
Total Number of Services configured	Total number of SLB services configured on the ACOS device.
Service	Real server name, service protocol port, and transport protocol (TCP or UDP).
State	Current state of the service: • Up • Down • Disabled
Persistent-Conn	Number of connections sent to the server by the persistence feature.

Example The following command shows Smart NAT statistics:

```
ACOS(config-slb vserver-vport)# show slb server rs auto-nat-
stats
Total Number of Services configured on Server rs: 21
Service    HA/VR ID  IP_RR Nat Address  Port Usage Total Used
Total Freed  Failed
-------------------------------------------------------------
----------------------
rs:80/tcp       1    Yes 10.212.1.225   64   660469 660405 0
                         10.212.1.226   64   660470 660406 0
rs:8080/tcp 1        Yes 10.212.1.225   0    0      0      0

                         10.212.1.226   0    0      0      0
```

In this example, all the virtual ports are using Smart NAT along with round-robin of floating IPs. The Nat Address, Port Usage, Total Used, Total Freed, and Failed columns show the same information shown in show IP NAT pool statistics output. (See the *CLI Reference*.)

The Service column lists the server, protocol port, and Layer 4 protocol. The HA/VR ID column lists the HA group ID or VRRP-A VRID, if applicable. In this example, the ACOS device is deployed as a standalone device, so "0" is shown in this column.

The following table describes the fields in the command output.

Field	Description
Service	Real server name and port number, and the Layer 4 protocol (TCP or UDP).
HA/VR ID	The HA group ID or VRRP-A VRID, if applicable.
NAT Address	The IP address used for the NAT mapping.
Port Usage	Number of mappings currently in use by sessions.
Total Used	Total number of sessions that have been NATted for the source address.
Total Freed	Number of NATted sessions that have been terminated, thus freeing up a port for another session.

Field	Description
Failed	Number of times a mapping attempt failed. Generally, this type of error occurs if the system does not have any resources for new mappings.

Example

The following example output shows a list of server bindings:

```
ACOS# show slb server bindings
Total Number of Servers configured: 24
Total Number of Services configured: 35
Service          Port  Address             State
-----------------------------------------------------------------
-----
rs1              8080  20.20.20.20
+sg-8080                                   All Up
  +=>vip2            10.10.10.200:8080
+linux:8080                                Functional Up
  +=>ITA-VIP-01      192.168.19.120:8080
```

NOTE: When two IP addresses are registered for the FQDN, and one is UP while the other is DOWN, the status is Functional UP.

This example shows server bindings for server “rs1”.

The service groups are indicated by “+”. In this example, the server is a member of the following service groups:

- sg-8080
- linux:8080

The VIP bindings are indicated by “+=>”. In this example, “rs1” has the following bindings:

- Bound to “vip2” through service group “sg-8080”
- Bound to “ITA-VIP-01” through service group “linux:8080”

The state of each service group is shown. In this example, service group “sg-8080” is All Up. This indicates all service ports on all real servers in the service group are up. Service group “linux:8080” is Functionally Up. The service is up on at least one real server in the service group, but not on all the servers in the group.

The following command displays the IP NAT statistics for SLB server.

```
ACOS (config)# show slb server rs ip-nat-stats
Total Number of Services configured on Server rs: 2
Service          Pool       Address      Port Usage Total Used Total
Freed  Failed
-------------------------------------------------------------------
------
rs:21/tcp        ipv4-pool3 10.212.1.243    0        2          2
0
                                      10.212.1.244     0        0
        0        0
```

Field	Description
Total Number of Services configured on Server	Number of services configured on SLB server.
Service	Real server name and port number, and the Layer 4 protocol (TCP or UDP).
Pool	The IP NAT Pool ID.
Address	The IP address used for the NAT mapping.
Port Usage	Number of mappings currently in use by sessions.
Total Used	Total number of sessions that have been NAT ed for the source address.
Total Freed	Number of NAT ed sessions that have been terminated, thus freeing up a port for another session.
Failed	Number of times a mapping attempt failed. Generally, this type of error occurs if the system does not have any resources for new mappings.

show slb service-group

Description Show SLB service-group information.

Syntax

```
show slb service-group [group-name] [brief] [config]
[all-partitions | partition {shared | name}] [link-cost-
statistics]
```

Parameter	Description
group-name	Shows information only for the specified service group. If you omit this option, information is shown for all service groups configured on the ACOS device.
brief	Shows a summary view of the configured service groups and their operational status. If you specify a service-group name, summary information is displayed for only that group. Otherwise, summary information for all groups is displayed.
config	Shows the SLB configuration of the service groups.
all-partitions	Show SLB service group information in all partitions.
partition	Show SLB service group information in the specified partition only.
link-cost-statistics *start_date end_date*	Show server group link-cost statistics (including cost estimate) for the specified duration. Mention the start date and end date. **NOTE:** The command **acos-events logdb enable-link-cost** needs to be configured in order to get the correct cost estimate for the specified duration.

Mode All

Example The following command shows statistics for SLB service groups:

```
ACOS# show slb service-group
                    Current = Current Connections, Total =
Total Connections
```

```
                    Fwd-p = Forward packets, Rev-p = Reverse
packets
                    Peak-c = Peak connections
Service Group Name
Service               Current Total    Fwd-p      Rev-p      Peak-
c
-------------------------------------------------------------------
-------
*sg-80-1     State: Down
rs-http:80               0      0         0          0          0

*sg-80-2     State: All Up
rs-http-2:80             1      1         1          4          5
```

The following table describes the fields in the command output.

Field	Description
Number of Service Groups configured	Total number of SLB service groups configured on the ACOS device.
Service Group Name	Name of the service group.
State	Indicates the state of the service group: • All Up – All service ports on all real servers in the service group are up. • Functional Up – Each service port number is up on at least one real server in the service group. • Down – Either all service ports are down, or some (not all) are Disabled. • Disabled – All the service ports are disabled.
Current	Current number of connections to the service.
Total	Number of connections to the service.
Fwd-p	Number of request packets received by the ACOS device for the service.

Field	Description
Rev-p	Total number of server response packets sent to clients by the ACOS device on behalf of real servers.
Peak-c	Peak connection count. Note: Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see extended-stats (individual server) and extended-stats (global).

Example

The following command shows configuration information and statistics for SLB service group “louis”:

```
ACOS# show slb service-group louis
Service group name: louis State: Disb
Service selection fail drop: 2
Service selection fail reset: 1
Service peak connection:          0
Priority affinity: 10
Service: s-4-2-1:80 DOWN
Request packets: 6 Response packets: 0
Request bytes: 360 Response bytes: 0
Current connections: 2 Persistent connections: 0
Current requests: 0 Total requests: 0
Total connections: 3 Response time: 0.00 msec
Total requests succ: 0
Peak conn:    0
Service: s-2-2-1:80 DOWN
Forward packets: 12 Reverse packets: 9
Forward bytes: 951 Reverse bytes: 396
Current connections: 0 Persistent connections: 0
Current requests: 0 Total requests: 0
Total connections: 3 Response time: 0.00 msec
Total requests succ: 0
Peak conn:    0
```

The following table describes the fields in the command output.

NOTE: A separate set of health check fields appears in the show slb service-group command output for HTTP traffic.

Field	Description
Service group name	Name of the service group.
State	Indicates the state of the service group: • All Up – All service ports on all real servers in the service group are up. • Functional Up – Each service port number is up on at least one real server in the service group. • Partially Up – Some service ports are up but others are down. • Down – Either all the service ports are down, or some but not all of them are Disabled. • Disabled – All the service ports are disabled.
Service selection fail drop	Number of server selection failures where the ACOS device dropped the client request.
Service selection fail reset	Number of server selection failures for which the ACOS device sent a RST to the client.
Service peak connection	Peak number of connections.
Priority affinity	Number associated with the currently active priority level. By default, the primary service-group members with the highest priority are active and appear in the output. However, if failover occurs, then the priority of the lower-priority secondary members appears in the output.
Service	Service bound to the service group. Also indicates the state of the service.

Field	Description
Forward packets	Total number of request packets received by the ACOS device for the service.
Reverse packets	Total number of server response packets sent to clients by the ACOS device on behalf of real servers.
Forward bytes	Total number of request bytes received by the ACOS device for the service.
Reverse bytes	Total number of server response bytes sent to clients by the ACOS device on behalf of real servers.
Current connections	Current number of connections to the service.
Persistent connections	Number of connections established on the server due to an SLB persistence feature.
Current requests	Current number of HTTP requests being processed by the server. In this field and the Total Requests and Total requests success fields, Layer 7 requests are counted only if Layer 7 request accounting is enabled using enable-l7-req-acct
Total requests	Total number of HTTP requests processed by the server.
Total connections	Total number of connections to the service.
Response time	Server response time.
Total requests succ	Total number of HTTP requests that were successful.
Peak conn	Peak connection count. Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see extended-stats (individual server) and extended-stats (global).

Example The following command shows configuration information for SLB service groups:

```
ACOS# show slb service-group config
slb service-group sg1 tcp
     member s1 80
!
slb service-group sg2 tcp
     member s2 80
     member s1 80
!
slb service-group sg3 tcp
     member s3 80
!
```

Example The following command shows configuration information for named SLB service groups:

```
ACOS (config-slb svc group)# show slb service-group sg config
Service group name: sg
Type: tcp                                Distribution: Svc Wtd RR
Health Check: None
Member Count: 2
Member2: s:80                            Priority: 1
Member1: s2:80                           Priority: 1
```

In this example, 2 service groups are configured. Each service group takes the weight from the service group member. It reuses the weight from the service member of the real server port number.

Example The following command displays a brief, summarized display of service-group information for all service groups:

```
ACOS# show slb service-group brief
Total Number of Service Groups configured: 2
slb service-group rontest tcp
Service group name: rontest
Type: tcp                          Distribution: Round Robin
Health Check: None
Servers Up = 0
Servers Down = 1
Servers Disabled = 0
```

```
Total Servers in Group = 1
slb service-group udptest udp
Service group name: udptest
Type: udp                          Distribution: Round Robin
Health Check: None
Servers Up = 0
Servers Down = 1
Servers Disabled = 0
Total Servers in Group = 1
```

In this example, 2 service groups are configured. Each service group has 1 server. In each of the groups, the server is down.

Example

The following sample command includes the **sort-priority** option that displays the members of a service group organized by their configured priority in descending order. For example, the **western-region** service group specified in the following example includes three members that are displayed in descending numeric order by priority (8, 4, then 1):

```
ACOS# show slb service-group western-region config sort-
priority
Service group name: western-region
Type: tcp                          Distribution: Round Robin
Health Check: None
Member Count:3
Member3: GW:80                     Priority: 8
Member2: FW1_Inspect:80            Priority: 4
Member1: DEFAULT_GATEWAY:80        Priority: 1
```

If you issue the command without the **sort-priority** option, the service group members appear in ascending alphabetical order (D, F, then G) as shown:

```
Member1: DEFAULT_GATEWAY:80        Priority: 1
Member2: FW1_Inspect:80            Priority: 4
Member3: GW:80                     Priority: 8
```

Example

The following command displays link-cost statistics for a server group, for the specified duration:

```
ACOS (config)# show slb service-group sg link-cost-statistics
2020-05-01 2020-06-01
Link Name     Link         Total Bytes     Interval        Average
             Max
              selected     Transferred     Transferred
Throughput(Kbpi)     Throughput(Kbpi)
-------------------------------------------------------------------
-------------------------
rs            0            0               50              1
              17
rs2           25439        10088300        124             1
              160
rs3           3011         1193928         67              1
              17

Estimated cost for dates 2020-05-01 - 2020-06-01: 2494
```

The following table describes the fields in the command output:

Field	Description
Link Name	The name of the selected link
Link Selected	The number of times the server link was selected
Total Bytes Transferred	Total Bytes transferred during the specified time
Interval Transferred	Total Bytes transferred during the current interval
Average Throughput	Average throughput (Kbpi) during the interval
Max Throughput	Maximum throughput (Kbpi) during the interval

show slb sip

Description Display SIP SLB statistics.

Syntax

```
show slb sip [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows SIP SLB statistics:

```
ACOS# show slb sip
                              Total
-------------------------------------------------------------------
----
SIP Session created             0
SIP Session freed               0
Curr SIP Proxy                  0
Total SIP Proxy                 0
Client message received         0
  Sent to server                0
  Incomplete                    0
  Drop                          0
  Connecting server             0
  Failed                        0
Server message received         0
  Sent to client                0
  Incomplete                    0
  Drop                          0
  Failed                        0
Server conn created             0
  Created successfully          0
  Failed                        0
```

The following table describes the fields in the command output.

Field	Description
SIP Session created	Total number of SIP sessions created.
SIP Session freed	Total number of SIP connection freed.
Curr SIP Proxy	Current number of SIP connections between the

Field	Description
	ACOS device and SIP servers.
Total SIP Proxy	Total number of SIP connections between the ACOS device and SIP servers.
Client message received	Total number of SIP messages received from clients: • Sent to server — Number of SIP messages received from client and forwarded to server. • Incomplete — Number of packet which contains incomplete message. • Drop — Number of packets dropped. • Connecting server — Client message currently in server connecting state. • Failed — Number of SIP messages received from clients not forwarded to servers.
Server message received	Total number of SIP messages received from servers: • Sent to client — Number of SIP messages received from server and forwarded to client. • Incomplete — Number of packet which contains incomplete message. • Drop — Number of SIP messages received from servers that were not forwarded to clients.
Server conn created	Total number of connections made with servers: • Created successfully — Number of successful connections. • Failed — number of failed connections.

show slb smpp

Description Display Short Message Peer-to-Peer (SMPP) protocol SLB statistics.

Syntax

```
show slb smpp [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows SMPP SLB statistics.

```
ACOS(config)# show slb smpp
                                Total
-------------------------------------------------------------
----
Curr SMPP Proxy                 0
Total SMPP Proxy                0
Client message received         0
  Sent to server                0
  Incomplete                    0
  AX responds directly          0
  Drop                          0
  Connecting server             0
  Failed                        0
Server message received         0
  Sent to client                0
  Incomplete                    0
  Drop                          0
  Failed                        0
Server conn created             0
  Created successfully          0
  Failed                        0
Client conn selection           0
    Select by request           0
    Select by roundbin          0
    Select by conn              0
    Select failed               0
Server conn selection           0
    Select by request           0
    Select by roundbin          0
    Select by conn              0
    Select failed               0
```

The following table describes the fields in the command output.

Field	Description
SMPP msg mem allocated	Total amount of memory currently in use for SMPP connections.
SMPP msg mem cached	Total amount of memory cached for SMPP connections.
SMPP msg mem freed	Total amount of memory freed after an SMPP connection has closed.
SMPP msg payload allocated	Total amount of memory allocated for the SMPP packet payload.
SMPP msg payload freed	Total amount of memory freed from the SMPP packet payload.
Curr SMPP Proxy	Number of currently active connections using the SMPP proxy.
Total SMPP Proxy	Total number of connections that have used the SMPP proxy.
Client message received	Total number of SMPP messages received from clients. • Sent to server – Number of SMPP messages received by the client and forwarded to the server. • Incomplete – Number of packets which contain incomplete messages. • AX responds directly – Number of times the ACOS device responded directly to a client's request. • Drop – Number of packets dropped due to the configured SMP resource limit. • Connecting server – Number of times the ACOS

Field	Description
	device forwarded a client's request to the SMPP server. • Failed – The following counters display the number of failed connections, listed by the cause: ◦Failed to parse ◦Failed to process ◦Failed to SNAT ◦Exceeded buff ◦Failed to send ◦Server conn start failed
Server message received	Total number of SMPP messages received from servers. • Sent to client – Number of SMPP messages received by the server and forwarded to the client. • Incomplete – Number of packets which contain incomplete messages. • Drop – Number of packets dropped due to the configured SMP resource limit. • Failed – Number of SMPP messages received by the server that were not forwarded to the client. The following counters display the number of failed connections, listed by cause: ◦Failed to parse ◦Failed to process ◦Failed to sel client conn ◦Failed to SNAT

Field	Description
	◦Exceeded buff ◦Failed to send
Server conn created	• Created successfully – Number of server connections created successfully. • Failed – Number of failed server connection attempts, listed by cause: ◦ Failed to SNAT ◦ Failed to construct ◦ Failed to reserve ◦ Failed to start ◦ Server conn already exists ◦ Failed to insert
Message parsing failed	Number of SMPP messages that the ACOS failed to parse. The following sub-counters describe the cause: • The packet size too small – Number of SMPP messages that were not parsed because the message size was less than 4 bytes. • Invalid sequence number – SMPP messages are incremented by +1. This counter indicates the total number of SMPP messages that were not parsed because of an incorrect sequence number.
Message processing failed	Number of times the ACOS could not process the SMPP message. The following sub-counters describe the cause: • No virtual port– There was no virtual port that matched the destination of the SMPP message. • Failed to select server – Server selection failure

Field	Description
	to forward the SMPP request.
Client conn selection	The following counters apply to SMPP client selection: • Select by request – Number of client connections, selected by the type of request message. • Select by roundbin – Number of client connection selected by the Round Robin algorithm. • Select by conn – Number of client connections, selected by the connection type. • Select failed – Number of times the ACOS failed to select a client for the SMPP connection.
Server conn selection	The following counters apply to SMPP server selection: • Select by request – Number of server connections, selected by the type of request message. • Select by roundbin – Number of server connection selected by the Round Robin algorithm. • Select by conn – Number of server connections, selected by the connection type. • Select failed – Number of times the ACOS failed to select a server for the SMPP connection.
Bind client and server	Number of times the ACOS successfully forwarded the initial BIND message from a client an SMPP server.
Unbind client and server	Number of times the ACOS disconnected the client to an SMPP server.

Field	Description
Receive enquire_link	Total number of ENQUIRE_LINK messages that the ACOS received from the SMPP client or server.
Receive enquire_link_ resp	Total number of ENQUIRE_LINK_RESP messages that the ACOS received from the SMPP client or server.
Send enquire_link	Total number of ENQUIRE_LINK messages that the ACOS device has sent.
Send enquire_link_ resp	Total number of ENQUIRE_LINK_RES messages that the ACOS device has sent.
Fail to bind server	Total number of times the ACOS device received a BIND message and failed to connect the client to an SMPP server.
Single message	Total number of single messages that were sent to the ACOS and did not require a response.
Transfer msg from L4 to L7 CPU	Number of SMPP messages that the ACOS transferred from a Layer 4 CPU to a Layer 7 CPU.
Fetch msg from L7 CPU	Number of SMPP messages that the ACOS transferred from the Layer 7 CPU to a Layer 4 CPU.
Transfer msg from proxy to conn CPU	Number of SMPP messages that the ACOS transferred from the proxy CPU to the connection CPU.
Fetch msg from conn CPU	Number of SMPP messages that the ACOS transferred from the connection CPU to the proxy CPU.
Transfer msg from L7 to L4 CPU	Number of SMPP messages that the ACOS transferred from a Layer 7 CPU to a Layer 4 CPU.
Transfer msg from conn to proxy CPU	Number of SMPP messages that the ACOS transferred from the connection CPU to the proxy CPU.

Field	Description
Alloc mem failed	Number of times a connection failed because the ACOS device did not have access to sufficient memory resources.
Unexpected error	Number of unexpected errors that are not categorized by the other counters.
AX holds msg	Number of messages that the ACOS device has received from a client or server and has yet to forward.
Splited packet	Number of times the ACOS split TCP packets which contain multiple SMPP messages.
Message in pipeline	Number of SMPP messages that the ACOS processed using an HTTP pipeline.
Client RST	Number of times TCP connections with clients were reset.
Server RST	Number of times TCP connections with servers were reset.

show slb smtp

Description Shows SLB information for SMTP. Insert server name to display SLB information for SMTP proxy server.

Syntax

```
show slb smtp [prxy_name  <1-65535>] [detail]
```

Parameter	Description
prxy_name <1-65535>	SMTP proxy server name and port number.
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows summary SMTP SLB statistics:

```
ACOS# show slb smtp
                            Total
-------------------------------------
```

```
Current proxy conns       0
Total proxy conns         0
SMTP requests             0
SMTP requests (success)   0
No proxy error            0
Client reset              0
Server reset              0
No tuple error            0
Parse request failure     0
Server selection failure  0
Forward request failure   0
Forward REQ data failure  0
Request retransmit        0
Request pkt out-of-order  0
Server reselection        0
Server premature close    0
Server connection made    0
Source NAT failure        0
Init server starttls       0
Real server starttls disable 0
Server starttls fail       0
```

The following table describes the fields in the command output.

Field	Description
Current proxy conns	Number of currently active SMTP connections using ACOS device as an SMTP proxy.
Total proxy conns	Number of SMTP connections that have used the ACOS device as an SMTP proxy.
SMTP requests	Total number of SMTP requests received by the SMTP proxy.
SMTP requests (success)	Number of SMTP requests received by the ACOS device that were successfully fulfilled (by connection to a real server).
No proxy error	Number of proxy errors.
Client reset	Number of times TCP connections with clients were

Field	Description
	reset.
Server reset	Number of times TCP connections with servers were reset.
No tuple error	Number of tuple errors.
Parse request failure	Number of times parsing of an SMTP request failed.
Server selection failure	Number of times selection of a real server failed.
Forward request failure	Number of forward request failures.
Forward REQ data failure	Number of forward request data failures.
Request retransmit	Number of retransmitted requests.
Request pkt out-of-order	Number of request packets received from clients out of sequence.
Server reselection	Number of times a request was forwarded to another server because the current server was failing.
Server premature close	Number of times the connection with a server closed prematurely.
Server connection made	Number of connections made with servers.
Source NAT failure	Number of source NAT failures.

Field	Description
Init server starttls	Number of STARTTLS sessions initiated with the server.
Real server starttls disable	Number of times the server was unable to negotiate a STARTTLS session.
Server starttls fail	Number of times a server STARTTLS session failed due to a TCP error event.

Example

This command shows detailed SMTP SLB statistics for each data processor (DP):

```
ACOS# show slb smtp detail
                          DP0         DP1         DP2
Total
-------------------------------------------------------------------
----
Current proxy conns       0           0           0           0
Total proxy conns         0           0           0           0
SMTP requests             0           0           0           0
SMTP requests (success)   0           0           0           0
No proxy error            0           0           0           0
Client reset              0           0           0           0
Server reset              0           0           0           0
No tuple error            0           0           0           0
Parse request failure     0           0           0           0
Server selection failure  0           0           0           0
Forward request failure   0           0           0           0
Forward REQ data failure  0           0           0           0
Request retransmit        0           0           0           0
Request pkt out-of-order  0           0           0           0
Server reselection        0           0           0           0
Server premature close    0           0           0           0
Server connection made    0           0           0           0
Source NAT failure        0           0           0           0
```

show slb source-port-rate-limit

Description Displays rate limiting of reset packets for unknown connection.

Syntax

```
show slb source-port-rate-limit
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb source-port-rate-limit
                                        Total
------------------------------------------------------------------
----
Curr src port entry                     0
Curr src port-ip entry                  0
Total alloc                             0
Total free                              0
Total rate exceed drop                  0
Total rate exceed reset                 0
Total log sent                          0
```

Field	Description
Curr src port entry	Number of current source port entries.
Curr src port-ip entry	Number of current source port-IP entries.
Total alloc	Total number of source port rate limit entries allocated.
Total free	Total number of source port rate limit entries freed.
Total rate exceed drop	Total number packets dropped due to rate limit being exceeded.
Total rate exceed reset	Total number of packets reset due to rate limit being exceeded.
Total log sent	Total number of logs sent for rate limit events.

show slb spdy-proxy

Description Show statistics for SLB SPDY proxy.

Syntax

```
show slb spdy-proxy [debug] [detail]
```

Parameter	Description
debug	Show debug information.
detail	Show statistics per CPU in the output.

Mode All

Example Sample output for this command:

```
ACOS# show slb spdy-proxy
                          Total
--------------------------------------
Curr Proxy Conns          0
Total Proxy Conns         0
Curr HTTP Proxy Conns     0
Total HTTP Proxy Conns    0
Version 2 Streams         0
Version 3 Streams         0
Curr Streams              0
Total Streams             0
Streams(succ)             0
Server RST sent           0
Server GOAWAY sent        0
TCP sock error            0
Inflate context           0
Deflate context           0
PING sent                 0
STREAM not found          0
Client FIN                0
Server FIN                0
Stream close              0
Session close             0
Stream err                0
Session err               0
Control frame received    0
```

```
      SYN stream            0
      SYN reply             0
      RST                   0
      Setting               0
      Ping                  0
      Goaway                0
      Headers               0
      Window update         0
Data frame received         0
Dt no stream found          0
Dt no stream & goaway       0
Dt no str&gw & cl ses       0
Est callback no tuple       0
Dat callback no tuple       0
Contex alloc fail           0
FIN close session           0
Serv RST close stream       0
Stream found                0
Clse St ses not found       0
Clse St str not found       0
Clsing closed stream        0
Str cl session close        0
Clsing closed session       0
Max conc stream limit       0
Stream alloc fail           0
HTTP conn alloc fail        0
Req/Header alloc fail       0
NV tot len exceed           0
NV zero name length         0
NV ivld http version        0
NV connection               0
NV keep alive               0
NV proxy-connection         0
NV transfer encoding        0
NV no must have             0
Decompress fail             0
SYN after goaway            0
Stream id < previous        0
Str already exist           0
Unidirectional SYN          0
```

```
Syn reply alr received    0
Cl RST str not found      0
Win upd no str found      0
Invalid window size       0
Unknown control frame     0
Data on closed stream     0
Invalid frame size        0
Invalid version           0
Hdr after ses close       0
Compr ctx alloc fail      0
Header compress fail      0
HTTP data ses close       0
HTTP data str nt fnd      0
Clse Str not http-pr      0
Session needs reque       0
New Str aftr Ses del      0
HTTP fin str alr clsd     0
HTTP cl str alr clsd      0
HTTP err str alr clsd     0
HTTP hdr str alr clsd     0
HTTP data str alr clsd    0
```

show slb sshi

Description Displays the SSH Insight (SSHi) statistics.

Syntax

```
show slb sshi stats vserver_name port_num
```

Mode All

Example The following example displays sample output:

```
ACOS# show slb sshi
```

show slb switch

Description Show SLB switching statistics.

Syntax

```
show slb switch [detail | ethernet port-num [detail]]
```

Parameter	Description
detail	Shows statistics per individual CPU in the output.
ethernet *port-num*	Shows statistics only for the specified Ethernet port.

Mode All

Example The following command shows summary SLB switching statistics:

```
ACOS# show slb switch
                          Total
-----------------------------------------------------------------
----
L2 Forward                2793
L3 IP Forward             0
IPv4 No Route Drop        0
L3 IPv6 Forward           0
IPv6 No Route Drop        0
L4 Process                709223
Incorrect Len Drop        0
Prot Down Drop            289
Unknown Prot Drop         32136
TTL Exceeded Drop         0
Link Down Drop            0
SRC Port Suppresion       0
VLAN Flood                141022
IP Fragment received      0
ARP REQ received          80272
ARP RESP received         15939
Forward Kernel            91163
IP(TCP) Fragment received0
IP Fragment Overlap       0
IP Frag Overload Drops    0
IP Fragment Reasm OKs     23
IP Fragment Reasm Fails   0
IP Fragment Timeout       0
Anomaly Land Attack Drop  0
Anomaly IP OPT Drops      0
Anomaly PingDeath Drop    0
```

```
Anomaly All Frag Drop     0
Anomaly TCP noFlag Drop   0
Anomaly SYN Frag Drop     0
Anomaly TCP SYNFIN Drop   0
Anomaly Any Drops         0
BPDUs Received            0
BPDUs Sent                0
ACL Denys                 0
SYN rate exceeded Drop    0
Packet Error Drops        0
IPv6 Frag UDP             0
IPv6 Frag TCP             0
IPv6 Frag ICMP            0
IPv6 Frag OSPF            0
IPv6 Frag ESP             0
IPv6 Frag Reasm OKs       0
IPv6 Frag Reasm Fails     0
IPv6 Frag Invalid Pkts    0
Bad Pkt Drop              0
IP Frag Exceed Drop       0
IPv4 No L3 VLAN FWD Drop  0
IPv6 No L3 VLAN FWD Drop  0
L2 Default Vlan FWD Drop  507865
BW Limit Drop             0
License Expire Drop       0
L4 Misc Er                0
Management Service Drop   0
Jumbo Frag Drop           0
IPv6 Jumbo Frag Drop      0
```

The following table describes the fields in the command output:

Field	Description
L2 Forward	When the ACOS device is acting as a Layer-2 switch and receives a packet that has the destination MAC address in its MAC table, ACOS sends the packet to the outgoing interface (as per the MAC table entry) and increments this counter.

Field	Description
L3 IP Forward	Number of packets that have been Layer 3 routed.
IPv4 No Route Drop	Number of IPv4 packets that were dropped due to routing failures.
L3 IPv6 Forward	Number of IPv6 packets that have been Layer 3 routed.
IPv6 No Route Drop	Number of IPv6 packets that were dropped due to routing failures.
L4 Process	Number of packets that went to a VIP or NAT for processing.
Incorrect Len Drop	Number of packets dropped due to incorrect protocol length. **NOTE:** A high value for this counter can indicate a packet length attack.
Prot Down Drop	• Number of IPv6 packets received on an interface for which there was no IPv6 address configured. • Number of IPv4 packets received on an interface for which there was no IPv4 address configured.
Unknown Prot Drop	Number of times ACOS dropped a packet because the packet was not one of the following: IPv4, IPv6, or ARP
TTL Exceeded Drop	Number of packets dropped due to TTL expiration.
Link Down Drop	Number of packets dropped because the outgoing link was down.
SRC Port Suppression	Number of packets dropped because the source and destination interface within the same VLAN is same.
VLAN Flood	Number of times ACOS received a packet that did not have the destination MAC address in the MAC table, causing ACOS to flood the packet out all other interfaces on the VLAN.

Field	Description
IP Fragment received	Number of IPv4 fragments that have been received.
ARP REQ received	Number of ARP requests the ACOS device received.
ARP RESP received	Number of ARP responses the ACOS device received in response to an ARP request sent by itself.
Forward Kernel	When the ACOS device receives a health monitor packet (for example, LACP or ARP packets), ACOS forwards these packets to the kernel for processing and increments this counter.
IP(TCP) Fragment received	Number of IP TCP fragments received.
IP Fragment Overlap	Number of overlapping fragments received.
IP Frag Overload Drops	Number of fragments dropped due to overload.
IP Fragment Reasm OKs	Number of successfully reassembled IP fragments.
IP Fragment Timeout	Number of times ACOS device does not receive subsequent fragments for fragmentation reassembly.
IP Fragment Reasm Fails	Number of IP fragment reassembly failures.
Anomaly Land Attack Drop	Number of SYN packets dropped because they were spoofed (used the destination IP address as the source IP address).
Anomaly IP OPT Drops	Number of packets dropped because they had IP options set.
Anomaly PingDeath Drop	Number of oversized (longer than 32 K) ICMP packets dropped.

Field	Description
	An oversized ICMP packet can trigger Denial of Service (DoS), crashing, freezing, or rebooting.
Anomaly All Frag Drop	Number of IP fragments dropped.
Anomaly TCP noFlag Drop	Number of TCP packets dropped because they had no flags set. TCP packets are normally sent with at least one bit in the flags field set.
Anomaly SYN Frag Drop	Number TCP SYN fragments dropped that had the fragmentation bit set. A SYN fragment attack floods the target host with SYN packet fragments. An unprotected host will store the fragments, in order to reassemble them. By not completing the connection, and flooding the server or host with such fragmented SYN packets, the attacker can cause the host's memory buffer to fill up eventually.
Anomaly TCP SYNFIN Drop	Number of TCP packets dropped that had TCP SYN *and* FIN bits set. An attacker can send a packet with both bits set to determine what kind of system reply is returned, and then use the system information for further attacks using known system vulnerabilities. Also, some older devices will let such packets through even though there is an established ACL defined and the state of the TCP connection is not considered to be established.
Anomaly Any Drops	Total number of packets dropped by IP anomaly filtering.
BPDUs Received	Number of Bridge Protocol Data Units (BPDUs) received.

Field	Description
BPDUs Sent	Number of Bridge Protocol Data Units (BPDUs) sent.
ACL Denys	Number of times traffic was not forwarded due to a deny rule in an Access Control List (ACL). This counter also includes traffic dropped due to the l3-vlan-fwd-disable action in ACL rules.
SYN rate exceeded Drop	Number of packets dropped because the TCP SYN threshold had been exceeded.
Packet Error Drops	Number of times the ACOS device dropped a packet due to a TCP/UDP checksum error.
IPv6 Frag UDP	Number of IPv6 UDP fragments received by the ACOS device.
IPv6 Frag TCP	Number of IPv6 TCP fragments received by the ACOS device.
IPv6 Frag ICMP	Number of IPv6 ICMP fragments received by the ACOS device.
IPv6 Frag OSPF	Number of IPv6 OSPF fragments received by the ACOS device.
IPv6 Frag ESP	Number of IPv6 ESP fragments received by the ACOS device.
IPv6 Frag Reasm OKs	Number of successfully reassembled IPv6 fragments.
IPv6 Frag Reasm Fails	Number of IPv6 fragment reassembly failures.
IPv6 Frag Invalid Pkts	Number of IPv6 fragments that were invalid.
Bad Pkt Drop	Number of bad packets dropped; this is a cumulative number for all packets that could not be processed (for example, packet has an incorrect length).
IP Frag Exceed Drop	Number of fragmented IP packets that were dropped because they exceeded the allowed maximum.

Field	Description
IPv4 No L3 VLAN FWD Drop	Number of IP packets that were dropped by the l3-vlan-fwd-disable action in an IPv4 ACL.
IPv6 No L3 VLAN FWD Drop	Number of IP packets that were dropped by the l3-vlan-fwd-disable action in an IPv6 ACL.
L2 Default VLAN FWD Drop	Number of times The DLF packets were dropped because the ACOS is configured to disallow flooding on the default VLAN (VLAN1).
BW Limit Drop	Number of packets dropped because they exceeded the bandwidth limit.
License Expire Drop	Number of packets dropped due to an invalid license.
L4 Misc Er	Number of Layer 4 packets dropped due to miscellaneous errors.
Management Service Drop	Number of times management traffic was drop because the specific service type was not enabled.
Jumbo Frag Drop	Number of dropped fragmented IPv4 jumbo packets.
IPv6 Jumbo Frag Drop	Number of dropped fragmented IPv6 jumbo packets.

Example

The following command shows detailed SLB switching statistics for Ethernet port 1:

```
ACOS# show slb switch ethernet 1 detail
DP0         DP1         DP2         Total
-------------------------------------------------------------
-
L2 Forward                2115        227         453         2795
L3 IP Forward             0           0           0           0
IPv4 No Route Drop        0           0           0           0
...
```

show slb syn-cookie

Description Show SLB hardware SYN-cookie statistics

Syntax

```
show slb syn-cookie
```

Mode All

show slb syn-cookie-buffer

Description Show SYN-cookie buffer statistics.

Syntax

```
show slb syn-cookie-buffer
```

Mode All

Example The following command shows SYN-cookie buffer information:

```
ACOS# show slb syn-cookie-buffer
Maximum SYN cookie buffer size  : 10
Total SYN cookie buffer queued  : 0
Total SYN cookie buffer drop    : 0
```

show slb tcp stack

Description Show statistics for TCP SLB.

Syntax

```
show slb tcp stack [detail]
```

Parameter	Description
detail	Show statistics per CPU in the output.

Mode All

Example The following command shows summary TCP stack statistics:

```
ACOS# show slb tcp stack
Total
-----------------------------------------------------------------
----
```

```
Currently EST conns       29
Active open conns         6968
Passive open conns        7938
Connect attemp failures   0
Total in TCP packets      678804
Total out TCP packets     712974
Retransmited packets      359
Resets received on EST conn  5369
Reset Sent                4303
```

The following table describes the fields in the command output.

Field	Description
Currently EST conns	Current number of established TCP connections being handled by the proxy.
Active open conns	Number of active connections open.
Passive open conns	Number of passive connections open.
Connect attemp failures	Number of TCP connection attempts that failed.
Total in TCP packets	Total number of TCP packets received by the TCP proxy.
Total out TCP packets	Total number of TCP packets sent by the TCP proxy.
Retransmitted packets	Number of TCP packets retransmitted by the TCP proxy.
Resets received on EST conn	Number of TCP Resets received for established connections.
Reset Sent	Number of TCP Resets sent by the ACOS device.
TCPIP out noroute	Number of times request failed to send due to route failure.

Example The following command shows summary TCP stack statistics when proxy header is configured:

```
ACOS#show slb tcp stack extend  | section Proxy
Proxy header v1                           1
Proxy header v2                           0
!
```

show slb template policy forward-policy-stats

Description Displays statistics for the configured forward policies like Explicit Proxy (EP/TP) for HTTP, SSL Policy and so on.

Mode All

Example The policy template defines what actions are applied to upstream traffic by the client-facing virtual server on the ACOS device. A configuration of this policy template follows:

```
slb template policy Explicit_Proxy
  forward-policy
    action Permit_to_Internet
      forward-to-internet FW1_Inspect_SG snat Internet_Pool
log
    source Any_Source
      match-any
      destination any action Permit_to_Internet
```

Example The statistics for the policy template `Explicit_Proxy` follow:

```
ACOS# show slb template policy forward-policy-stats

slb template policy name: Explicit_Proxy
Source NAT failure:                       0
Unresolved DNS requests:                  0
Outstanding DNS requests:                 0
Hits:                                     2
Requests forward to Internet:             0
Requests forward to Service Group:        0
Requests forward to Proxy:                0
Requests dropped:                         1
Source Match not found:                   0
Expected Client HELLO requests not found:0
```

```
ACOS(config)#show slb template policy forward-policy-stats

slb template policy name: HTTP-POLICY
Source NAT failure:                              0
Unresolved DNS requests:                         0
Outstanding DNS requests:                        0
Hits:                                            0
Requests forward to Internet:                    0
Requests forward to Service Group:               0
Requests forward to Proxy:                       0
Requests dropped:                                0
Source Match not found:                          0
Expected Client HELLO requests not found:        0

slb template policy name: SSL-POLICY
Source NAT failure:                              0
Unresolved DNS requests:                         0
Outstanding DNS requests:                        0
Hits:                                            0
Requests forward to Internet:                    0
Requests forward to Service Group:               0
Requests forward to Proxy:                       0
Requests dropped:                                0
Source Match not found:                          0
Expected Client HELLO requests not found:        0

slb template policy name: Explicit_Policy_SSLi
Source NAT failure:                              0
Unresolved DNS requests:                         0
Outstanding DNS requests:                        0
Hits:                                            0
Requests forward to Internet:                    0
Requests forward to Service Group:               0
Requests forward to Proxy:                       0
Requests dropped:                                0
Source Match not found:                          0
Expected Client HELLO requests not found:        0
```

Field	Description
slb template policy name	The name of the policy template the forward-policy is bound to.
Source NAT failure	The count of source NAT failures.
Unresolved DNS requests	The count of DNS requests for the IP address of the downstream server that could not be resolved.
Outstanding DNS requests	The current number of queued DNS requests.
Hits	The count of the matches to the source IP address specified in the forward-policy. When the client sends one HTTPS request, the Hits counter increases by '2' and the Request Dropped counter increases by '1'. This is because it includes two requests: CONNECT and an actual HTTPS request. The CONNECT request is forwarded by ACOS, but the HTTPS request is dropped. However, when the client sends one HTTP request, both the Hits and Request Dropped counters increases by 1.
Requests forward to Internet	Number hits that have been forwarded to the Internet URL requested by the clients.
Requests forward to Service Group	The count of hits that have been forwarded to service-group specified in the forward-policy.
Requests forward to Proxy	Number of hits forwarded to another HTTP proxy server in the forward-policy.
Requests	The count of client connection requests dropped.

Field	Description
dropped	
Source Match not found	Number of client connection requests where the source IP address could not be found.
Expected Client HELLO requests not found	The count of client connection requests in which the HELLO message was absent or could not be parsed.

show slb virtual-server

Description Show information for SLB virtual servers.

Syntax

```
show slb virtual-server [
virtual-server-name
   [vport-num
      {
      port-type [service-group-name] |
      [application-statistics [extended]] |
      detail | [dns]
      dns-cache {entry {all-entries | dns-class string | dns-
type string | domain-name {dns-domain-name | fqdn-domain}
name} }|
      host-hits-counter {host-name | all} |
      url-hits-counter {url-string | all}
      }
   ]
[bind]
[config]
[all-partitions]
[partition {shared | name}]
```

Option	Description
virtual-server-name	Shows information only for the specified virtual server. The *vport-num port-type* option shows information only for the specified virtual port on the virtual server.

Option	Description

	• The *service-group-name* option further restricts the output, to show information only for the specified service group.
	• The **application-statistics** option displays statistics related to an application.
	  ◦ **extended** - Displays the detailed statistics related to an application.
	• The **detail** option displays connection and packet statistics. Specifying **detail** also shows the connection rate per virtual port for each virtual server. For more information, see the examples below.
	• The option **dns-cache** along with **entry** display DNS cache entries for one of the filters given below:
	  ◦ **all-entries** - Displays all the cache entries without limiting the display to the default value of 10,000.
	  Note: If configured, the display of cache entries may take a longer time if the number of entries is large.
	  ◦ **dns-class** - You can specify one of the following DNS classes:
	  ◦ **IN** – INTERNET class
	  ◦ **CH** – CHAOS class
	  ◦ **HS** – HESIOD class
	  ◦ **NONE** – NONE class
	  ◦ **ANY** – ANY class
	  ◦ *num* - Other class value (1-65535)

Option	Description
	◦ **dns-type** - Specify one of the following DNS types: ◦ **A** – Address type ◦ **AAAA** – IPv6 Address type ◦ **CNAME** – Canonical name type ◦ **MX** – Mail exchange type ◦ **NS** – Name server type ◦ **SRV** – Service locator ◦ **PTR** – PTR resource type ◦ **SOA** – Start of authority type ◦ **TXT** – Text type ◦ **ANY** – All cached type ◦ *num* - Other type value (1-65535) ◦ **domain-name** - Specify one of the following options: ◦ **dns-domain-name** – Domain name ◦ **fqdn-domain** – Fully qualified domain name • The **host-hits-counter** option displays rule-matching statistics for host switching. Each time traffic matches a host-matching rule in an HTTP template, the applicable “hits” counter is incremented. • The **url-hits-counter** option displays rule-matching statistics for URL switching. Each time traffic matches a URL-switching rule in an HTTP template, the applicable “hits” counter is incremented.
all-partitions	Show information for all partitions.

Option	Description
bind	Includes the service groups and real servers and ports bound to the virtual ports.
config	Displays virtual-server configuration information. You can optionally specify the specific partition for which you want to view this configuration.
partition	Show information for a specific partition.

Mode All

Usage To display virtual-server information for a specific partition, use the **partition** option; use **partition shared** for the shared partition, or **partition** *name*, where *name* is a specific L3V partition.

Example The following command shows summary information for all virtual servers:

```
ACOS# show slb virtual-server
Total Number of Virtual Services configured: 2
Virtual Server Name      IP              Current    Total
Request  Response Peak
Service-Group            Service         connection connection
packets  packets  connection
-------------------------------------------------
*v-server(A)              3.1.1.99
   port 80  http                         0          3
14       10       611
abctcp                   80/http         0          2
14       10       2112
Total received conn attempts on this port: 3
   port 53  udp                          0          0
0        0        411
abcudp                   53/udp          0          0
0        0        696969
Total received conn attempts on this port: 0
...
```

The following table describes the fields in the command output.

Field	Description
Total Number of Virtual Services configured	Total number of virtual services (virtual server ports) configured on the ACOS device.
Virtual Server Name	Name of the virtual server. Underneath the virtual server name, each of the virtual ports on the server is listed, followed by the service groups in which the virtual server and the virtual port are members. In the example above, virtual server “v-server” has two virtual ports, HTTP port 80 and UDP port 53. HTTP port 80 is a member of service group “abctcp”, and UDP port 53 is a member of service group “abcudp”. For each VIP, its VRRP-A state on the ACOS device is shown by one of the following: • (A) – VIP is in active state on this ACOS device. • (S) – VIP is in standby state on this ACOS device. The primary servers are listed under the virtual port. If alternates are configured for a primary server, the alternates are listed under the primary server. If an asterisk is shown at the end of an alternate server name, the primary server is down and the alternate server is active instead.
IP	Virtual IP address of the virtual server.
Current connection	Current number of connections to the virtual service port.

Field	Description
	NOTE: Connection and packet counters are listed separately for virtual ports and for service groups.
Total connection	Total number of connections to the virtual service port.
Request packets	Number of request packets received for the virtual service.
Response packets	Number of server reply packets sent by the ACOS device for the virtual service.
Peak connection	Peak connection count. Note: Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see the following: • slb common (global) • extended-stats (individual virtual server) • extended-stats (individual virtual service port)
Total received conn attempts on this port	Total number of connection requests received for this port.
Service-Group	Service group bound to the virtual service.
Service	Virtual service port number and service type.

Example

This command shows status information for SLB virtual server “v-server”:

```
ACOS(config)# show slb virtual-server v-server
Virtual server: v-server   State: All Up IP: 3.1.1.99  Port
Curr-conn  Total-conn Rev-Pkt Fwd-Pkt   Peak-conn
-----------------------------------------------------------------
--------------------------------
```

```
Virtual Port:80 / service:abctcp / state:All Up port 80  http
0       3          10      14      1011
Source NAT Pool: pootest
Virtual Port:53 / service:abcudp / state:All Up port 53  udp
0       0          0       0       811
Source NAT Pool: pootest
Total Traffic                    0          3          10
   14        1822
...
```

The following table describes the fields in the command output.

Field	Description
Virtual server	Name of the virtual server.
State	State information is shown separately for virtual servers and for individual virtual ports. Virtual server state: • All Up – All virtual ports on the virtual server are Running. • Functional Up – Some of the virtual ports are Running or Functional Running, but at least one of them is not Running. • Partial Up – At least one virtual port is Running or Functional Running, but at least one other virtual port is Down. • Down – All the virtual ports are Down. • Disb – The virtual server has been administratively disabled. Virtual port state: • All Up – All members (real servers and ports) in all service groups bound to the virtual port are up. • Functional Up – At least one member in a service group

Field	Description
	bound to the virtual port is up, but not all members are up. • Down – All members in all service groups bound to the virtual port are down. • Disb – The virtual port has been administratively disabled.
IP	Virtual IP address of the virtual server.
Port	Virtual port number and service type.
Curr-conn	Current number of connections to the virtual service port.
Total-conn	Total number of connections to the virtual service port.
Rev-Pkt	Number of server reply packets sent by the ACOS device for the virtual service.
Fwd-Pkt	Number of request packets received for the virtual service.
Peak-conn	Peak connection count. **NOTE:** Peak connection statistics are collected only if the extended-stats option is enabled. To enable extended-stats, see the following: • slb common (global) • extended-stats (individual virtual server) • extended-stats (individual virtual service port)

Example The following command shows configuration information:

```
ACOS# show slb virtual-server config
Total Number of Virtual Services configured: 1
Virtual server Name              Address
-----------------------------------------------
louis2                       192.168.20.253
```

```
member0:louis                  80/http
Source NAT Pool: p1 HTTP Template: clientip-insert
Reuse Template: cr  Persist Cookie:cookie-persist aFleX:
bugzilla_proxy_fix
```

The following table describes the fields in the command output.

Field	Description
Total Number of Virtual Services configured	Total number of virtual services (virtual server ports) configured on the ACOS device.
Virtual server Name	Name of the virtual server.
Address	Virtual IP address of the virtual server.
member	Real server bound to the virtual server. The number at the end is assigned by the ACOS device for this show command output. Under the member name, the NAT pools and SLB templates bound to the virtual server are listed.

Example

The following command shows configuration information for named SLB service groups:

```
ACOS(config-slb svc group)# show slb virtual-servicer vip 80
http
Service group name: sg
Type: tcp                                Distribution: Svc Wtd RR
Health Check: None
Member Count: 2
   Pri       Port/State              Curr-conn  Total-conn
Rev-Pkt    Fwd-Pkt   Peak-conn
-----------------------------------------------------------------
------------------------------
1               s:80/Up                  0          0          0          0
1               s2:80/Up                 0          0          0          0
Virtual Port Traffic                     0          0          0
0        1822
```

In this example, 2 service groups are configured. Each service group takes the weight from the service group member. It reuses the weight from the service member of the real server port number.

Example

The following command shows details for a virtual server:

```
ACOS# show slb virtual-server vip1 detail
Virtual server name:                              vip1
Virtual server IP address:
200.200.200.100
Virtual server MAC:                               021f:a000:0000
Virtual server template:                          adi
Connection rate limit:                          800000 per second
Connection rate over limit action:              drop
Current connection:                               24254
Current request:                                  0
Total connection:                                 3024486
Total request:                                    0
Total request success:                            0
Total forward bytes:                              2561556963
Total forward packets:                            42249486
Total reverse bytes:                              286542491
Total reverse packets:                            75962845
Peak connections:                                    0
Current connection rate:                          121 per second
```

The following table describes the fields in the command output.

Field	Description
Virtual server name	Name of the virtual server.
Virtual server IP address	IP address of the virtual server.
Virtual server MAC	MAC address of the VIP.
Virtual server template	Name of the virtual server template bound to the virtual server.
Current	Current number of connections to the virtual port.

Field	Description
connection	
Current request	Current number of HTTP requests being processed by the virtual port. NOTE: In this field and the Total request and Total request success fields, Layer 7 requests are counted only if Layer 7 request accounting is enabled. See slb common.
Current response	Current number of HTTP responses being processed by the virtual port.
Total connection	Total number of connections that have been made to the virtual port.
Total request	Total number of HTTP requests processed by the virtual port.
Total response	Total number of HTTP respnses processed by the virtual port.
Total request success	Total number of HTTP requests that were successful.
Total response success	Total number of HTTP responses that were successful.
Total forward bytes	Number of request bytes forwarded to the virtual port.
Total forward packets	Number of request packets forwarded to the virtual port.
Total reverse bytes	Number of request bytes received from the virtual port.
Total reverse packets	Number of request packets received from the virtual port.
Peak connections	Peak connection count. Peak connection statistics are collected only if the

Field	Description
	extended-stats option is enabled. To enable extended-stats, see the following: • slb common (global) • extended-stats (individual virtual server) • extended-stats (individual virtual service port)
Current connection rate	Current connection rate for the virtual port on the virtual server.
Current request rate	Current request rate for the virtual port on the virtual server.
Current response rate	Current response rate for the virtual port on the virtual server.

Example

The following command shows details for a virtual port on a virtual server:

```
ACOS(config)# show slb virtual-server vip1 80 detail
Virtual port name:                              vip1:80:tcp
Virtual port number:
220.220.220.100:80
Virtual port template:                          default
Current connection:                             11216
Current request:                                0
Current response:                               0
Total connection:                               6215984
Total request:                                  0
Total response:                                 0
Total request success:                          0
Total response success:                         0
Total forward bytes:                            51614803
Total forward packets:                          80370519
Total reverse bytes:                            3536281441
Total reverse packets:                          39742461
Peak connections:                               0
Response time:                                  1
Fastest Rsp time:                               1
```

```
Slowest Rsp time:                                    1
Current connection rate:                             268 per second
Current request rate:                                0 per second
Current response rate:                               0 per second
```

The following table describes the fields in the command output.

Field	Description
Virtual port name	Name of the virtual server, virtual port, and port type.
Virtual port number	IP address of the virtual server and protocol port number of the virtual port.
Virtual port template	Name of the virtual port template bound to the virtual port.
Current connection	Current number of connections to the virtual port.
Current request	Current number of HTTP requests being processed by the virtual port. In this field and the Total request and Total request success fields, Layer 7 requests are counted only if Layer 7 request accounting is enabled. See slb common.
Total connection	Total number of connections that have been made to the virtual port.
Total request	Total number of HTTP requests processed by the virtual port.
Total request success	Total number of HTTP requests that were successful.
Total forward bytes	Number of request bytes forwarded to the virtual port.
Total forward packets	Number of request packets forwarded to the virtual port.
Total reverse bytes	Number of request bytes received from the virtual port.

Field	Description
Total reverse packets	Number of request packets received from the virtual port.
Peak connections	Peak connection count. NOTE: Peak connection statistics are collected only if the **extended-stats** option is enabled. To enable extended-stats, see the following: • slb common (global) • extended-stats (individual virtual server) • extended-stats (individual virtual service port)
Current connection rate	Current connection rate for the virtual port on the virtual server.

Example The following command shows service group and port bindings:

```
ACOS# show slb virtual-server bind
------------------------------------------------------------------
-------------------
*Virtual Server : SanJose(A)              192.192.100.100 Down

    +port 80  tcp ====>sg-80-1                    State :Down
+rs-http:80                       192.168.215.16       State :
Down

*Virtual Server : Chicago(A)              192.192.200.200 All
Up

    +port 80  tcp ====>sg-80-2                    State :All Up
+rs-http-2:80                     192.168.215.13       State :
Up
```

In this example, virtual port 80 on virtual server SanJose is bound to real port 80 on real server rs-http in service group sg-80-1. Likewise, virtual port 80 on virtual server Chicago is bound to real port 80 on real server rs-http-2 in service group sg-80-2.

For each VIP, its VRRP-A state on the ACOS device is shown by one of the following:

- (A) – VIP is in active state on this ACOS device.
- (S) – VIP is in standby state on this ACOS device.

Example

The following example shows the information displayed if alternate (backup) servers are configured:

```
ACOS(config)# show slb virtual-server bind
Total Number of Virtual Services configured: 1
------------------------------------------------------------------
-------------------
*Virtual Server : http-with-alternates(A)
192.168.10.10 Functional Up

    +port 80  http ====>http1                              State
:Functional Up
        +rs1:80                          10.10.10.10
State : Up
   Alternate: rs1-a1, rs1-a2, rs1-a3
        +rs2:80                          10.10.10.20
State : Down
   Alternate: rs2-a1*, rs2-a2, rs2-a3
```

The primary servers are listed under the virtual port. Under each primary server, that server's alternate servers are listed.

If an asterisk is shown at the end of an alternate server name, the primary server is down and the alternate server is active instead. In the example above, rs2 is down, so alternate rs2-a1 is being used instead.

Example

The following example demonstrates the DNS statistics displayed for a virtual server:

```
ACOS(config)# show slb virtual-server v1 53 dns-tcp
application-statistics
Total DNS Query: 0
Total Malformed Query: 0
DNS Response Rate Limiting Total Allowed: 0
DNS Response Rate Limiting Total Dropped: 0
DNS Response Rate Limiting Total Slipped: 0
```

```
DNS Response Rate Limiting Bad FQDN: 0
Total DNS Filter Query Type Drop: 0
Total DNS Filter Query Class Drop:       0
DNS Filter Query Type A Drop: 0
DNS Filter Query Type AAAA Drop: 0
DNS Filter Query Type CNAME Drop: 0
DNS Filter Query Type MX Drop: 0
DNS Filter Query Type NS Drop: 0
DNS Filter Query Type SRV Drop: 0
DNS Filter Query Type PTR Drop: 0
DNS Filter Query Type SOA Drop: 0
DNS Filter Query Type TXT Drop: 0
DNS Filter Query Type ANY Drop: 0
DNS Filter Query Type OTHERS Drop: 0
DNS Filter Query Class INTERNET Drop: 0
DNS Filter Query Class CHAOS Drop: 0
DNS Filter Query Class HESIOD Drop: 0
DNS Filter Query Class NONE Drop: 0
DNS Filter Query Class ANY Drop: 0
DNS Filter Query Class OTHERS Drop: 0
DNS Recursive Resolution Started:        0
DNS Recursive Resolution Succeeded:       0
DNS RPZ Action Drop: 0
DNS RPZ Action Pass Through: 0
DNS RPZ Action Force Switching TCP: 0
DNS RPZ Action NXDOMAIN Return: 0
DNS RPZ Action NODATA Return: 0
DNS RPZ Action Walled Garden: 0
DNS RPZ Trigger Client IP: 0
DNS RPZ Trigger Response IP: 0
DNS RPZ Trigger NS IP: 0
DNS RPZ Trigger QNAME: 0
DNS RPZ Trigger NS Domain Name: 0
```

Example The following example demonstrates the DNS statistics in http virtual port displayed for a virtual server:

NOTE: The level counters increment only when DNS template is bound to DoH template.

```
ACOS(config)# show slb virtual-server v1 443 https
application-statistics dns
Total DNS Request Received:                         0
Total DNS Response Received:                        0
Total DNS Drop:                                     0
Request Drop:                                       0
Request Sent:                                       0
Response Generated:                                 0
Response Sent:                                      0
Response Drop:                                      0
Request Timeout:                                    0
Cache Hit:                                          0
Response Rate Limiting Total Allowed:               0
Response Rate Limiting Total Dropped:               0
Response Rate Limiting Total Slipped:               0
Response Rate Limiting Bad FQDN:                    0
Request Retransmit:                                 0
Total Malformed Query:                              0
Malformed Drop:                                     0
Query Too Long Drop:                                0
Query Filter Drop:                                  0
Total DNS Filter Query Type Drop:                   0
Total DNS Filter Query Class Drop:                  0
GSLB Drop:                                          0
GSLB Query Drop:                                    0
GSLB Malformed Query:                               0
GSLB Response Drop:                                 0
GSLB Malformed Response:                            0
GSLB Query Forwarded:                               0
GSLB Response Forwarded:                            0
GSLB Response Received:                             0
RPZ Action Drop:                                    0
RPZ Action Pass Through:                            0
RPZ Action Force Switching TCP:                     0
RPZ Action NXDOMAIN Return:                         0
RPZ Action NODATA Return:                           0
RPZ Action Walled Garden:                           0
RPZ Trigger Client IP:                              0
RPZ Trigger Response IP:                            0
RPZ Trigger NS IP:                                  0
```

```
RPZ Trigger QNAME:                              0
RPZ Trigger NS Domain Name:                     0
Recursive Resolution Started:                   0
Recursive Resolution Succeeded:                 0
Recursive Resolution Send Failed:               0
Recursive Resolution Timed Out:                 0
Recursive Resolution Retransmit Sent:           0
Recursive Resolution Retransmit Exceeded:       0
Recursive Resolution Buffer Alloc Failed:       0
Recursive Resolution ongoing Client retransmit: 0
Recursive Resolution not dplane:                0
Recursive Resolution no resolver:               0
Recursive Resolution Max Trials Exceeded:       0
Recursive Resolution no Hints:                  0
Recursive Resolution Res submit err:            0
Recursive Resolution Res check err:             0
Recursive Resolution UDP Conn Err:              0
Recursive Resolution TCP Conn Err:              0
Recursive Resolution UDP Snd Fail:              0
Recursive Resolution ICMP Err:                  0
Recursive Resolution Query Not Sent:            0
Client SSL Success:                             0
Server SSL Success:                             0
Backend UDP Connections Created:                0
Backend UDP Conn Established:                   0
Paddings to Server Stripped:                    0
Paddings to Client Added:                       0
Edns Client Subnet to Server Removed:           0
Edns Client Subnet Received:                    0
Edns Client Subnet Inserted:                    0
UDP Retransmission:                             0
UDP Retransmission Failed:                      0
```

Example

The following example displays the statistics per virtual port of DNSSEC validation done through recursive resolution:

```
ACOS(config)#sh slb virtual-server vs 53 dns-udp application-
statistics
Total DNS Request Received:                     0
Total DNS Response Received:                    0
...
```

```
Recursive Resolution Total trials max:          0
Recursive Resolution Reach max Depth:           0
Recursive Resolution DNSSEC-OK Req Received:    0
Recursive Resolution DNSSEC-OK Resp Served:     0
Recursive Resolution DNSSEC Validation Failed:  0
Recursive Resolution Late Responses:            0
Recursive Resolution Parallel Queries UDP:      6
RR DNSSEC Validation Algorithm not Supported:   0
RR DNSSEC Validation Digest Type not Supported: 0
RR DNSSEC Validation RRSIG Signer Name Err:     0
RR DNSSEC Validation RRSIG Labels Err:          0
RR DNSSEC Validation RRSIG non Validity Period: 0
RR DNSSEC Validation DNSKEY Protocol Err:       0
RR DNSSEC Validation Incorrect Signature:       0
RR DNSSEC Validation Incorrect Key Digest:      0
RR DNSSEC Validation with Trust Anchor Failed:  0
RR DNSSEC Validation RRSet Size Exceed Limit:   0
Client SSL Success:                             0
```

Example The following example displays the statistics of DNS queries based on web categories:

```
ACOS(config)#show slb virtual-server vip 53 dns-udp
application-statistics | inc Category
Category Action Drop:                           0
Category Action Respond:                        2
Category Action Permit:                         0
Category Respond NXDomain:                      0
Category Respond No Answer:                     0
Category Respond Type A:                        1
Category Respond Type AAAA:                     0
Category Respond Type CNAME:                    1
Category Bypass:                                0
Category Async Request Sent (Template + aFlex): 1
Category Async Result (Template + aFlex):       1
Category No Local No Lookup (Template + aFlex): 0
```

The following table describes the fields in the command output.

Field	Description
Category Action Drop	Number of categorized DNS queries that were dropped.
Category Action Respond	Number of categorized DNS queries that were responded.
Category Action Permit	Number of categorized DNS queries that were allowed.
Category Respond NXDomain	Number of responses sent for queries c (NXDOMAIN).
Category Respond No Answer	Number of responses with no answer available for the queried domain.
Category Respond Type A	Number of type A responses returned in the DNS query response.
Category Respond Type AAAA	Number of type AAAA responses returned in the DNS query response.
Category Respond Type CNAME	Number of type CNAME responses returned in the DNS query response.
Category Bypass	Number of DNS requests bypassed during web category lookup.
Category Async Request Sent (Template + aFlex)	Number of DNS requests sent to the Webroot's server when the queries are not found in the local database. This counter is a sum of requests made from an SLB DNS template and an aFleX script.
Category Async Result (Template +	Number of DNS requests, for which a result is received from the Webroot server. This counter is a sum of requests made from an SLB DNS template

Field	Description
aFlex)	and an aFleX script.
Category No Local No Lookup (Template + aFlex)	Number of DNS requests not found in the local database, with online lookup not configured. This counter is a sum of requests made from an SLB DNS template and an aFleX script.

Example

The following example displays the extended statistics for the SLB virtual server configured for handling DNS traffic over UDP:

```
ACOS#show slb virtual-server vip 53 dns-udp application-
statistics extended
Total DNS Response Received:                    0
Total DNS Drop:                                 0
Request Drop:                                   0
Request Sent:                                   9
Response Generated:
Response Sent:                                  2
Response Drop:                                  0
Request Timeout:                                0
TC Response Sent Due to max-udp-size:           0
Response Rate Limiting Total Allowed:           0
Response Rate Limiting Total Dropped:           0
Response Rate Limiting Total Slipped:           0
Response Rate Limiting Total TC:                0
Response Rate Limiting Bad FQDN:                0
Request Retransmit:                             0
Total Malformed Query:                          0
Malformed Drop:                                 0
Query Too Long Drop:                            0
Query Filter Drop:                              0
Total DNS Filter Query Type Drop:               0
Total DNS Filter Query Class Drop:              0
RPZ Action Drop:                                0
RPZ Action Pass Through :                       0
RPZ Action Force Switching TCP:                 0
RPZ Action NXDOMAIN Return:                     0
RPZ Action NODATA Return:                       0
RPZ Action Walled Garden:                       0
```

```
RPZ Trigger Client IP:                          0
RPZ Trigger Response IP:                        0
RPZ Trigger NS IP:                              0
RPZ Trigger QNAME:                              0
RPZ Trigger NS Domain Name:                     0
Recursive Resolution Send Failed:               0
Recursive Resolution Timed Out:                 0
Recursive Resolution Retransmit Sent:           0
Recursive Resolution Retransmit Exceeded:       0
Recursive Resolution Buffer Alloc Failed:       0
Recursive Resolution ongoing Client retransmit: 0
Recursive Resolution not dplane:                0
Recursive Resolution no resolver:               0
Recursive Resolution Max Trials Exceeded:       0
Recursive Resolution no Hints:                  0
Recursive Resolution Invalid Hints:             0
Recursive Resolution Res submit err:            0
Recursive Resolution Res check err:             0
Recursive Resolution UDP Conn Err:              0
Recursive Resolution TCP Conn Err:              0
Recursive Resolution UDP Snd Fail:              0
Recursive Resolution ICMP Err:                  0
Recursive Resolution Query Not Sent:            0
Recursive Resolution Response Truncated:        0
Recursive Resolution TC Response Received:      0
Recursive Resolution Serving Full Response:     0
Recursive Resolution NS Cache missing Glue:     0
Recursive Resolution NS Cache entry hit:        0
Recursive Resolution NS Cache entry miss:       0
Recursive Resolution Full Cache Response:       0
Recursive Resolution Pending Resolution:        0
Recursive Resolution Query Dropped:             0
Recursive Resolution Respond With Servfail:     0
Recursive Resolution Late Responses:            0
Recursive Resolution Parallel Queries UDP:      2
Recursive Resolution Parallel Queries TCP:      0
Recursive Resolution Total trials 1:            0
Recursive Resolution Total trials 3:            1
Recursive Resolution Total trials 6:            1
Recursive Resolution Total trials 12:           0
```

```
Recursive Resolution Total trials 24:           0
Recursive Resolution Total trials 48:           0
Recursive Resolution Total trials 64:           0
Recursive Resolution Total trials 128:          0
Recursive Resolution Total trials max:          0
Recursive Resolution Reach max Depth:           0
Client SSL Success:                             0
Server SSL Success:                             0
Backend UDP Connections Created:                0
Backend UDP Conn Established:                   0
UDP Retransmission:                             0
UDP Retransmission Failed:                      0
DNS TCP Pipeline Request Drop:                  0
Category Action Drop:                           0
Category Action Respond:                        0
Category Action Permit:                         0
Category Respond NXDomain:                      0
Category Respond No Answer:                     0
Category Respond Type A:                        0
Category Respond Type AAAA:                     0
Category Respond Type CNAME:                    0
Category Bypass:                                0
===Extended Statistics===
Query Type A:                                   2
Query Type AAAA:                                0
Query Type CNAME:                               0
Query Type MX:                                  0
Query Type NS:                                  0
Query Type SRV:                                 0
Query Type PTR:                                 0
Query Type SOA:                                 0
Query Type TXT:                                 0
Query Type ANY:                                 0
Query Type RRSIG:                               0
Query Type TSIG:                                0
Query Type DNSKEY:                              0
Query Type AXFR:                                0
Query Type IXFR:                                0
Query Type CAA:                                 0
Query Type NAPTR:                               0
```

```
Query Type DS:
Query Type CERT:                                0
Query Type HTTPS:                               0
Query Type other type:                          0
Rcode FORMERR Received:                         0
Rcode SERVERERR Received:                       0
Rcode NXDOMAIN Received:                        0
Rcode NOTIMPL Received:                         0
Rcode REFUSE Received:                          0
Rcode YXDOMAIN Received:                        0
Rcode YXRRSET Received:                         0
Rcode NXRRSET Received:                         0
Rcode NOTAUTH Received:                         0
Rcode NOTZONE Received:                         0
Rcode DSOTYPEN Received:                        0
Rcode OTHER VALUE Received:                     0
EDNS Query Type NSID:                           0
EDNS Query Type DAU:                            0
EDNS Query Type N3U:                            0
EDNS Query Type EXPIRE:                         0
EDNS Query Type COOKIE:                         2
EDNS Query Type KEEPALIVE:                      0
EDNS Query Type PADDING:                        0
EDNS Query Type CHAIN:                          0
EDNS Rcode BADVER Received:                     0
EDNS Rcode BADKEY Received:                     0
EDNS Rcode BADTIME Received:                    0
EDNS Rcode BADMODE Received:                    0
EDNS Rcode BADNAME Received:                    0
EDNS Rcode BADALG Received:                     0
EDNS Rcode BADTRANC Received:                   0
EDNS Rcode BADCOOKIE Received:                  0
Empty Response Received:                        0
===Device Generate===
Rcode NOERROR Generated:                        0
Rcode FORMERR Sent:                             0
Rcode SERVERERR Sent:                           0
Rcode NXDOMAIN Sent:                            0
Rcode NOTIMPL Sent:                             0
Rcode REFUSE Sent:                              0
```

```
Rcode YXDOMAIN Sent:                          0
Rcode YXRRSET Sent:                           0
Rcode NXRRSET Sent:                           0
Rcode NOTAUTH Sent:                           0
Rcode DSOTYPEN Sent:                          0
Rcode OTHER VALUE Sent:                       0
EDNS Rcode BADVER Sent:                       0
EDNS Rcode BADKEY Sent:                       0
EDNS Rcode BADTIME Sent:                      0
EDNS Rcode BADMODE Sent:                      0
EDNS Rcode BADNAME Sent:                      0
EDNS Rcode BADALG Sent:                       0
EDNS Rcode BADTRANC Sent:                     0
EDNS Rcode BADCOOKIE Sent:                    0
Filter Query Type A Drop:                     0
Filter Query Type AAAA Drop:                  0
Filter Query Type CNAME Drop:                 0
Filter Query Type MX Drop:                    0
Filter Query Type NS Drop:                    0
Filter Query Type SRV Drop:                   0
Filter Query Type PTR Drop:                   0
Filter Query Type SOA Drop:                   0
Filter Query Type TXT Drop:                   0
Filter Query Type ANY Drop:                   0
Filter Query Type OTHERS Drop:                0
Filter Query Class INTERNET Drop:             0
Filter Query Class CHAOS Drop:                0
Filter Query Class HESIOD Drop:               0
Filter Query Class NONE Drop:                 0
Filter Query Class ANY Drop:                  0
Filter Query Class OTHERS Drop:               0
```

The following table describes the fields in the command output for extended statistics:

Field	Description
Total DNS Response Received	Total number of DNS responses received from server.

Field	Description
Total DNS Drop	Total number of DNS packets dropped (query & response).
Request Drop	Number of DNS requests dropped.
Request Sent	Number of DNS requests forwarded to backend server.
Response Generated	Number of DNS responses generated.
Response Sent	Number of DNS responses forwarded to client.
Response Drop	Number of DNS responses dropped.
Request Timeout	Number of queries timed out when forwarding to server.
TC Response Sent Due to max-udp-size	Number of truncated (TC-flagged) UDP DNS responses sent because the responses exceeded the configured maximum UDP size limit.
Response Rate Limiting Total Allowed	Total number of responses allowed under rate limiting.
Response Rate Limiting Total Dropped	Total number of responses dropped due to rate limiting.
Response Rate Limiting Total Slipped	Total number of rate-limited responses that were slipped.
Response Rate Limiting Total TC	Total number of rate-limited responses with TC (truncated) flag.
Response Rate Limiting Bad FQDN	Total number of bad FQDNs triggering rate limiting.
Request Retransmit	Total number of retransmissions sent to DNS server.

Field	Description
Total Malformed Query	Total number of queries dropped due to being malformed.
Malformed Drop	Total number of drops for malformed DNS traffic (query and response).
Query Too Long Drop	Total number of DNS queries dropped due to size (max-query-length in DNS template).
Query Filter Drop	Total number of DNS queries dropped due to DNS template filter configuration.
Total DNS Filter Query Type Drop	Total DNS queries dropped due to DNS type filter.
Total DNS Filter Query Class Drop	Total DNS queries dropped due to DNS class filter.
RPZ Action Drop	Number of DNS queries dropped due to Response Policy Zone (RPZ) rules.
RPZ Action Pass Through	Number of queries allowed through without action due to RPZ rules.
RPZ Action Force Switching TCP	Number of queries forced to use TCP due to RPZ.
RPZ Action NXDOMAIN Return	RPZ rule caused DNS server to return NXDOMAIN.
RPZ Action NODATA Return	RPZ rule caused DNS server to return NODATA.
RPZ Action Walled Garden	RPZ redirected DNS query to a walled garden.
RPZ Trigger Client IP	RPZ policy triggered based on the client's IP address.

Field	Description
RPZ Trigger Response IP	RPZ policy triggered based on the IP address in the DNS response.
RPZ Trigger NS IP	RPZ rule triggered based on the nameserver's IP address.
RPZ Trigger QNAME	RPZ rule triggered by the queried domain name (QNAME).
RPZ Trigger NS Domain Name	RPZ policy triggered by the domain name of the nameserver (NS domain).
Recursive Resolution Send Failed	Number of times failure to send out query during recursive resolution.
Recursive Resolution Timed Out	Number of times timeout happened during recursive resolution.
Recursive Resolution Retransmit Sent	Number of times retransmission sent in case of timeout during recursive resolution.
Recursive Resolution Retransmit Exceeded	Number of times timeout happened but the retransmission times has reached the limit during recursive resolution.
Recursive Resolution Buffer Alloc Failed	Number of times failure to allocate packet buffer resources during recursive resolution.
Recursive Resolution ongoing Client retransmit	Number of times the retransmitted client DNS request is received while recursive resolution is still in progress.
Recursive Resolution not	Number of times the resolution skipped due to data plane constraints.

Field	Description
dplane	
Recursive Resolution no resolver	No resolver available for request.
Recursive Resolution Max Trials Exceeded	Number of times the number of outgoing queries has reached limit during recursive resolution.
Recursive Resolution no Hints	Root hints missing.
Recursive Resolution Invalid Hints	Number of times failure to get the hint during recursive resolution.
Recursive Resolution Res submit err	Number of times failure to allocate resolver resources during recursive resolution.
Recursive Resolution Res check err	Number of times all other errors happened during recursive resolution.
Recursive Resolution UDP Conn Err	Number of times errors regarding to UDP connection happened during recursive resolution.
Recursive Resolution TCP Conn Err	Number of times errors regarding to TCP connection happened during recursive resolution.
Recursive Resolution UDP Snd Fail	Number of times failure to send out UDP packet during recursive resolution.
Recursive Resolution ICMP Err	Number of times recursive resolution ends up sending ICMP error to client.

Field	Description
Recursive Resolution Query Not Sent	Number of times query failed to be sent.
Recursive Resolution Response Truncated	Number of times the response served from recursive resolution is truncated and has TC flag on.
Recursive Resolution TC Response Received	Number of times ACOS received a truncated (TC-flagged) DNS response during recursive resolution.
Recursive Resolution Serving Full Response	Number of times full DNS response is served to client.
Recursive Resolution NS Cache missing Glue	Number of times DNS cache of glue record is missing during NS cache lookup of recursive resolution.
Recursive Resolution NS Cache entry hit	Number of times DNS NS cache lookup hit and the cache is used in recursive resolution.
Recursive Resolution NS Cache entry miss	Number of times DNS NS cache lookup miss in recursive resolution.
Recursive Resolution Full Cache Response	Number of times DNS cache saved from recursive resolution is served with full response.
Recursive Resolution	When receives a DNS query but recursive resolution of same query is in progress.

Field	Description
Pending Resolution	
Recursive Resolution Query Dropped	When receives a DNS query but recursive resolution of same query is in progress, drop the query per configuration.
Recursive Resolution Respond With Servfail	When receives a DNS query but recursive resolution of same query is in progress, respond SERVFAIL response per configuration.
Recursive Resolution Late Responses	Responses received after timeout.
Recursive Resolution Parallel Queries UDP	UDP-based parallel recursive queries.
Recursive Resolution Parallel Queries TCP	TCP-based parallel recursive queries.
Recursive Resolution Total trials 1	Recursive resolution takes in total 1 outgoing query before done.
Recursive Resolution Total trials 3	Recursive resolution takes in total 2~3 outgoing queries before done.
Recursive Resolution Total trials 6	Recursive resolution takes in total 4~6 outgoing queries before done.
Recursive Resolution Total trials 12	Recursive resolution takes in total 7~12 outgoing queries before done.

Field	Description
Recursive Resolution Total trials 24	Recursive resolution takes in total 13~24 outgoing queries before done.
Recursive Resolution Total trials 48	Recursive resolution takes in total 25~48 outgoing queries before done.
Recursive Resolution Total trials 64	Recursive resolution takes in total 49~64 outgoing queries before done.
Recursive Resolution Total trials 128	Recursive resolution takes in total 65~128 outgoing queries before done.
Recursive Resolution Total trials max	Recursive resolution takes in total more than 128 outgoing queries before done.
Recursive Resolution Reach max Depth	Recursive resolution reaches the maximum support layers when resolving additional NS address or CNAME chain.
Client SSL Success	Number of client-side SSL connection established successfully.
Server SSL Success	Number of server-side SSL connection established successfully.
Backend UDP Connections Created	Number of backend UDP connection created.
Backend UDP Conn Established	Number of backend UDP connection established successfully.
UDP Retransmission	Number of backend UDP retransmission in case of timeout.
UDP	Number of backend UDP retransmission failure.

Field	Description
Retransmission Failed	
DNS TCP Pipeline Request Drop	Number of times error happen while DNS TCP proxy parses DNS packet that contains multiple requests in one packet.
Category Action Drop	Number of categorized DNS queries that were dropped.
Category Action Respond	Number of categorized DNS queries that were responded.
Category Action Permit	Number of categorized DNS queries that were allowed.
Category Respond NXDomain	Number of responses sent for queries category.
Category Respond No Answer	Number of responses with no answer available for the queried domain.
Category Respond Type A	Number of type A responses returned in the DNS query response.
Category Respond Type AAAA	Number of type AAAA responses returned in the DNS query response.
Category Respond Type CNAME	Number of type CNAME responses returned in the DNS query response.
Category Bypass	Number of DNS requests bypassed during web category lookup.
Query Type A	Number of DNS queries for type A.
Query Type AAAA	Number of DNS queries for type AAAA.

Field	Description
Query Type CNAME	Number of DNS queries for type CNAME.
Query Type MX	Number of DNS queries for type MX.
Query Type NS	Number of DNS queries for type NS.
Query Type SRV	Number of DNS queries for type SRV.
Query Type PTR	Number of DNS queries for type PTR.
Query Type SOA	Number of DNS queries for type SOA.
Query Type TXT	Number of DNS queries for type TXT.
Query Type ANY	Number of DNS queries for type ANY.
Query Type RRSIG	Number of DNS queries for type RRSIG.
Query Type TSIG	Number of DNS queries for type TSIG.
Query Type DNSKEY	Number of DNS queries for type DNSKEY.
Query Type AXFR	Number of DNS queries for type AXFR.
Query Type IXFR	Number of DNS queries for type IXFR.
Query Type CAA	Number of DNS queries for type CAA.
Query Type NAPTR	Number of DNS queries for type NAPTR.
Query Type DS	Number of DNS queries for type DS.
Query Type	Number of DNS queries for type CERT.

Field	Description
CERT	
Query Type HTTPS	Number of DNS queries for type HTTPS.
Query Type other type	Number of DNS queries for other type.
Rcode FORMERR Received	Number of DNS responses received indicating format error.
Rcode SERVERERR Received	Number of DNS responses received indicating server error.
Rcode NXDOMAIN Received	Number of DNS responses received indicating that the queried domain does not exist.
Rcode NOTIMPL Received	Number of DNS responses received indicating that the requested operation is not implemented.
Rcode REFUSE Received	Number of DNS responses received indicating refusal to perform the operation.
Rcode YXDOMAIN Received	Number of DNS responses received indicating that the requested operation could not be completed because the domain already exists.
Rcode YXRRSET Received	Number of DNS responses indicating that the requested operation could not be completed because the resource record set (RRset) already exists.
Rcode NXRRSET Received	Number of DNS responses received indicating that the requested operation could not be completed because the resource record set (RRset) does not exist.
Rcode NOTAUTH	Number of DNS responses received indicating that the server is not authoritative for the requested

Field	Description
Received	domain or operation.
Rcode NOTZONE Received	Number of DNS responses received indicating that the queried domain does not exist in the authoritative zone.
Rcode DSOTYPEN Received	Number of DNS responses received indicating that the requested DNSSEC signing algorithm or data signing type is not implemented or supported.
Rcode OTHER VALUE Received	Number of DNS responses received indicating the additional Rcode values are not explicitly defined by the standard DNS protocol.
EDNS Query Type NSID	Number of DNS queries having the NSID (Name Server Identifier) option.
EDNS Query Type DAU	Number of DNS queries having the DAU (DNSSEC Algorithm Understood) option.
EDNS Query Type N3U	Number of DNS queries having the N3U (NSEC3 Hash Understood.) option.
EDNS Query Type EXPIRE	Number of DNS queries having the Expire (Extension Mechanisms for DNS (EDNS) EXPIRE Option.) option set.
EDNS Query Type COOKIE	Number of DNS queries having the Cookie (Domain Name System (DNS) Cookies.) option.
EDNS Query Type KEEPALIVE	Number of DNS queries having the Keepalive (The edns-tcp-keepalive EDNS0 Option) option.
EDNS Query Type PADDING	Number of DNS queries having the Padding (The EDNS(0) Padding Option) option.
EDNS Query Type CHAIN	Number of DNS queries having the Chain (CHAIN Query Requests in DNS) option.
EDNS Rcode BADVER Received	Number of DNS responses received having EDNS Rcode set Bad OPT Version.

Field	Description
EDNS Rcode BADKEY Received	Number of DNS responses received having EDNS Rcode set key not recognized.
EDNS Rcode BADTIME Received	Number of DNS responses received having EDNS Rcode set signature out of time window.
EDNS Rcode BADMODE Received	Number of DNS responses received having EDNS Rcode set Bad TKEY Mode.
EDNS Rcode BADNAME Received	Number of DNS responses received having EDNS Rcode set duplicate key name.
EDNS Rcode BADALG Received	Number of DNS responses received having EDNS Rcode set algorithm not supported.
EDNS Rcode BADTRANC Received	Number of DNS responses received having EDNS Rcode set bad truncation.
EDNS Rcode BADCOOKIE Received	Number of DNS responses received having EDNS Rcode set bad/missing Server Cookie.
Empty Response Received	Number of DNS responses have no answer record.
Rcode NOERROR Generated	Number of DNS responses generated with no error (successful query).
Rcode FORMERR Sent	Number of DNS responses sent indicating format error.
Rcode SERVERERR Sent	Number of DNS responses sent indicating server error.

Field	Description
Rcode NXDOMAIN Sent	Number of DNS responses sent indicating that the queried domain does not exist.
Rcode NOTIMPL Sent	Number of DNS responses sent indicating that the requested operation is not implemented.
Rcode REFUSE Sent	Number of DNS responses sent indicating refusal to perform the operation.
Rcode YXDOMAIN Sent	Number of DNS responses sent indicating that the requested operation could not be completed because the domain already exists.
Rcode YXRRSET Sent	Number of DNS responses sent indicating that the requested operation could not be completed because the resource record set (RRset) already exists.
Rcode NXRRSET Sent	Number of DNS responses sent indicating that the requested operation could not be completed because the resource record set (RRset) does not exist.
Rcode NOTAUTH Sent	Number of DNS responses sent indicating that the server is not authoritative for the requested domain or operation.
Rcode DSOTYPEN Sent	Number of DNS responses sent indicating that the queried domain does not exist in the authoritative zone.
Rcode OTHER VALUE Sent	Number of DNS responses sent indicating that the requested DNSSEC signing algorithm or data signing type is not implemented or supported.
EDNS Rcode BADVER Sent	Number of DNS responses sent having EDNS Rcode set Bad OPT Version.
EDNS Rcode BADKEY Sent	Number of DNS responses sent having EDNS Rcode set key not recognized.
EDNS Rcode	Number of DNS responses sent having EDNS Rcode

Field	Description
BADTIME Sent	set signature out of time window.
EDNS Rcode BADMODE Sent	Number of DNS responses sent having EDNS Rcode set Bad TKEY Mode.
EDNS Rcode BADNAME Sent	Number of DNS responses sent having EDNS Rcode set duplicate key name.
EDNS Rcode BADALG Sent	Number of DNS responses sent having EDNS Rcode set algorithm not supported.
EDNS Rcode BADTRANC Sent	Number of DNS responses sent having EDNS Rcode set bad truncation.
EDNS Rcode BADCOOKIE Sent	Number of DNS responses sent having EDNS Rcode set bad/missing Server Cookie.
Filter Query Type A Drop	Number of A record queries dropped by filtering.
Filter Query Type AAAA Drop	Number of AAAA (IPv6) queries dropped.
Filter Query Type CNAME Drop	Number of CNAME record queries dropped.
Filter Query Type MX Drop	Number of mail exchange record queries dropped.
Filter Query Type NS Drop	Number of nameserver record queries dropped.
Filter Query Type SRV Drop	Number of service record queries dropped.
Filter Query Type PTR Drop	Number of pointer (reverse DNS) queries dropped.

Field	Description
Filter Query Type SOA Drop	Number of start-of-authority record queries dropped.
Filter Query Type TXT Drop	Number of text record queries dropped.
Filter Query Type ANY Drop	Number of ANY-type queries dropped.
Filter Query Type OTHERS Drop	Number of queries of other types not listed above that were dropped.
Filter Query Class INTERNET Drop	Number of internet (IN) class queries dropped.
Filter Query Class CHAOS Drop	Number of CHAOS class queries dropped.
Filter Query Class HESIOD Drop	Number of HESIOD class queries dropped.
Filter Query Class NONE Drop	Number of NONE class queries dropped.
Filter Query Class ANY Drop	Number of ANY class queries dropped.
Filter Query Class OTHERS Drop	Number of queries with unrecognized or other classes dropped.

Example

The following example displays the T2 counter added for the NXDOMAIN response rate limiting:

```
ACOS(config-dns-response-rate-limiting)# show slb virtual-
server VS 53 dns-udp application-statistics
...
...
RRL NXDOMAIN Exceed (Server-Side):                6
```

```
RRL QPS Drop / Log (Client-Side):                0
RRL NXDOMAIN Drop/ Log (Client-Side):            1
...
...
Response Rate Limiting Total Allowed:            0
Response Rate Limiting Total Dropped:            0
```

The following table describes the fields in the above command output:

Field	Description
RRL NXDOMAIN Exceed (Server-Side)	Number of NXDOMAIN responses that exceeded the configured rate limit on the server side.
RRL QPS Drop / Log (Client-Side)	Number of queries per second (QPS) responses dropped or logged on the client side that exceeded the configured rate limit on the client side.
RRL NXDOMAIN Drop/ Log (Client-Side)	Number of NXDOMAIN responses dropped or logged on the client side that exceeded the configured rate limit on the client side.
Response Rate Limiting Total Allowed	Total number of QPS and NXDOMAIN responses allowed within the configured rate limit.
Response Rate Limiting Total Dropped	Total number of QPS and NXDOMAIN responses dropped after the configured rate limit is exceeded.

Example

The following example demonstrates the DNS TCP statistics displayed for a virtual server:

```
ACOS(config)# show slb virtual-server vs1 53 dns-tcp
application-statistics
Total DNS Query: 0
First  set of 92 query
Total DNS Request Received:                      92
Total DNS Response Received:                     92
Total DNS Drop:                                  0
```

```
Request Drop:                                   0
Request Sent:                                   92
Response Generated:                             0
Response Sent:                                  92
Response Drop:                                  0
Request Timeout:                                0
Cache Hit:                                      0
```

Example The following example demonstrates the DNS UDP statistics displayed for a virtual server:

```
ACOS(config)#show slb virtual-server vs1 53 dns-udp
application-statistics
Total DNS Request Received:                     192
Total DNS Response Received:                    100
Total DNS Drop:                                 0
Request Drop:                                   0
Request Sent:                                   100
Response Generated:                             92
Response Sent:                                  192
Response Drop:                                  0
Request Timeout:                                0
Cache Hit:                                      92
```

The following table describes the fields in the above command output:

Field	Description
Total DNS Request Received	Total number of DNS requests received on the virtual server.
Total DNS Response Received	Total number of DNS responses received on the virtual server.
Total DNS Drop	Total number of DNS requests dropped on the virtual server.
Request Drop	Number of DNS requests dropped.
Request Sent	Number of DNS requests sent.
Response Generated	Number of DNS responses generated by the virtual server.

Field	Description
Response Sent	Number of DNS responses sent out to clients.
Response Drop	Number of DNS responses dropped on the virtual server.
Request Timeout	Number of DNS requests that timed out.
Cache Hit	Number of DNS responses served from the cache.

clear health https ssl-ticket

Description Clears all or specified HTTPS health monitor SSL session ticket cached in the PIN.

Syntax

```
clear health https ssl-tickets {health monitor name}
```

Mode Health monitor configuration

Example The following command configures clears all the health https SSL session ticket.

```
ACOS(config)# clear health https ssl-tickets
```

Example The following command manually clear the specified health https SSL session ticket.

```
ACOS(config)# clear health https ssl-tickets hm-https
```

clear slb unused-server-ports

Description Deletes real server ports that are not assigned to at least one service group by removing the corresponding port statements from slb real server configurations.

The system log displays ports that are deleted by the clear command.

Syntax

```
clear slb unused-server-ports [all-partitions]
```

The command is available in all partitions. The all-partitions option is only available in the shared partition and extends the command influence to all partitions on the device. When the all-partition option is not specified, the clear port action is effective only within the partition where it is invoked.

Block merge and replace modes do not support the removal of ports through this clear command. The system log provides a Warning message when the clear slb unused-server-port command is not successful.

Mode Privileged EXEC mode

Example The `clear slb unused-server-ports` command removes a tcp port (78) and udp port (98) from the s1 real server. The `show` commands demonstrate the effect of the `clear` command.

```
ACOS(config)# show running-config slb
!Section configuration: 378 bytes
!
slb server s1 10.0.0.15
  port 78 tcp
  port 88 tcp
  port 88 udp
  port 98 udp
  port 98 tcp
!
slb service-group sg1 tcp
  member s1 88
  member s1 98
!
slb service-group sg2 udp
  member s1 88
!
ACOS(config)# clear slb unused-server-ports
ACOS(config)# show running-config slb
!Section configuration: 333 bytes
!
slb server s1 10.0.0.15
  port 88 tcp
  port 88 udp
```

```
  port 98 tcp
!
slb service-group sg1 tcp
  member s1 88
  member s1 98
!
slb service-group sg2 udp
  member s1 88
!
ACOS(config)#
```

clear slb virtual-server

Description Clear information for SLB virtual servers.

Syntax

```
clear slb virtual-server [
virtual-server-name
   [vport-num
      {
      port-type [service-group-name] |
      [application-statistics] |
      [detail] |
      [dns-cache {entry {dns-class string | dns-type string |
domain-name {dns-domain-name | fqdn-domain} name}}] |
      host-hits-counter {host-name | all} |
      url-hits-counter {url-string | all}
      }
   ]
[all]]
```

Option	Description
virtual-server-name	Clear information only for the specified virtual server. • The *vport-num port-type* option clears information only for the specified virtual port on the virtual server. • The *service-group-name* option further restricts the output, to clear information only for the specified service group. • The option **application-statistics** clears statistics related to an application.

Option	Description
	• The **detail** option clears connection and packet statistics. Specifying **detail** also clears the connection rate per virtual port for each virtual server. • The option **dns-cache** along with **entry** clears DNS cache entries for one of the filters given below: ◦ **dns-class** - You can specify one of the following DNS classes: ◦ **IN** – INTERNET class ◦ **CH** – CHAOS class ◦ **HS** – HESIOD class ◦ **NONE** – NONE query class ◦ **ANY** – ANY query class ◦ *num* - Other class value (1-65535) ◦ **dns-type** - You can specify one of the following DNS types: ◦ **A** – Address type ◦ **AAAA** – IPv6 Address type ◦ **CNAME** – Canonical name type ◦ **MX** – Mail exchange type ◦ **NS** – Name server type ◦ **SRV** – Service locator ◦ **PTR** – PTR resource type ◦ **SOA** – Start of authority type ◦ **TXT** – Text type ◦ **ANY** – All cached type ◦ *num* - Other type value (1-65535)

Option	Description
	◦ **domain** - You can specify either one of the following ◦ **dns-domain-name** – Domain name ◦ **fqdn-domain** – Fully qualified domain name • The **host-hits-counter** option clears rule-matching statistics for host switching. • The **url-hits-counter** option clears rule-matching statistics for URL switching.
all	Clear information for all

Mode Privileged EXEC mode

Usage To clear the virtual-server information for a specific partition, use the **partition** option; use **partition shared** for the shared partition, or **partition** *name*, where *name* is a specific L3V partition.

Example The following command clears the virtual port DNS cache based on FQDN:

```
ACOS(config)# clear slb virtual-server vip1 53 dns-udp dns-cache entry domain-name fqdn-domain foo.com
```

Example The following command clears the virtual port DNS cache for DNS type ANY:

```
ACOS(config)# clear slb virtual-server vip1 53 dns-tcp dns-cache entry dns-type ANY
```

Example The following command clears the virtual port DNS cache for DNS class 66:

```
ACOS(config)# clear slb virtual-server vip1 53 dns-tcp dns-cache entry dns-class 66
```

Secure Socket Layer Insight

Thunder Secure Socket Layer Insight (SSLi) decrypts traffic across all ports, enabling third-party security devices to analyze all enterprise traffic without compromising performance. SSLi can detect and decrypt encryption on even non-proprietary TCP protocols. SSLi is deployable in a number of different ways, customizable for your network environment, with added HA. The integrated load balancing capability of SSLi helps to optimize the SSLi performance.

This reference lists the CLI configuration and show commands that apply specifically to SSLi.

Configuration Commands

slb template client-ssl

Description Names an SSL client template and enters the configuration mode where you can enable SSL client services, such as validation of SSL clients.

Syntax

```
[no] slb template client-ssl template-name
```

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters SLB Client-SSL Template Configuration mode.

Default If none of the SSL Client template sub-commands in the preceding table are configured, the default action of the SSL Client template is the combined default actions of the individual SSL C;lient sub-commands.

Mode Configuration mode

Usage The normal form of this command creates a client-SSL configuration template. The **no** form of this command removes the template.

For the **forward-proxy-bypass** option, match rules are always applied in the following order:

- **equals** *sni-string*
- **starts-with** *sni-string*
- **contains** *sni-string*
- **ends-with** *sni-string*

A client-SSL template can contain up to 128 certificates or certificate chains. They must be imported onto the ACOS device. To import a certificate or certificate chain, see import command.

You can bind only one client-SSL template to a virtual port. However, you can bind the same client-SSL template to multiple ports.

The **close-notify** option can not be used along with the TCP-proxy template **force-delete-timeout** option. Doing so may cause unexpected behavior

Example The following commands configure a client-SSL template named "client-ssl1" that uses imported CA certificates and requires clients to present their certificates when requesting connections to servers:

```
ACOS(config)# slb template client-ssl client-ssl1
ACOS(config-client ssl)# ca-cert ca-bundle.crt
ACOS(config-client ssl)# client-certificate require
```

Example These commands configure a client SSL template to use an imported CA certificate and key, and an imported Certificate Revocation List (CRL) from the CA:

```
ACOS(config)# slb template client-ssl client-ssl1
ACOS(config-client ssl)# ca-cert ca-cert.pem
ACOS(config-client ssl)# ca-cert ca-crl.pem
ACOS(config-client ssl)# client-certificate require
```

Example The following example shows how the certificate drop action is enabled in the SSL Client template named, **ClientSide_vRouter**. Specifically, the drop action occurs when OCSP reports the certificate is not currently valid.

```
ACOS-Inside(config)# slb template client-ssl ClientSide_
vRouter
ACOS-Inside(config-client ssl# forward-proxy-verify-cert-drop
```

Example

This example demonstrates the `forward-proxy-inspect` command. In this example of an AC class-list, all URLs ending with `private.abc.com` are bypassed, while all URLs ending with `public.abc.com` will go through SSLi processing.

```
ACOS# show config class-list
!Section configuration: 77 bytes
!
class-list my_class_list ac
  ends-with abc.com
  user-tag Security
!
ACOS# config
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# slb template client-ssl SSLi_vip_001_
client_ssl
ACOS(config-client ssl)# forward-proxy-inspect class-list my_
class_list
ACOS(config-client ssl)# forward-proxy-bypass contains
private.abc.com
```

auth-username

Description

Specifies the field to check in SSL certificates from clients in order to find the client name.

Syntax

```
[no] auth-username {
  [common-name]
  [subject-alt-name-email]
  [subject-alt-name-othername]
}
```

Parameter	Description
common-name	Configuring this option causes the ACOS device to extract the client's common name from the certificate.
subject-	Configuring this option causes the ACOS device to

Parameter	Description
alt-name-email	extract the Email address from the client's certificate. For example, if the client name is "user@example.com" then the entire string "user@example.com" would be extracted with this option
subject-alt-name-othername	Configuring this option causes the ACOS device to extract the UPN information from the certification. For example, if the client name is "user@example.com" then the string "user" would be extracted with this option.

Default The default is **common-name**.

Mode SLB client SSL template configuration mode

Usage Multiple options can be specified, but you must specify at least one.

If multiple options are specified, the ACOS device will attempt to extract the username from the options in the order they are specified. For example:

```
auth-username subject-alt-name-email subject-alt-name-othername
```

This command causes the ACOS device to first attempt to extract the username from **subject-alt-name-email**, and only if not found, will it then attempt to extract the username from **subject-alt-name-othername**.

Example Configure the ACOS device to extract the Email address from the client certificate:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# auth-username subject-alt-name-email
```

auth-username-attribute

Description Specify attribute name of username for client SSL.

Syntax

```
[no] auth-username-attribute string
```

Parameter	Description
string	Attribute name (1-31 characters).

Default None.

Mode SLB client SSL template configuration mode

Example Configure “username” as the username attribute name:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# auth-username-attribute username
```

authorization

Description Specify an LDAP server to user for client SSL authorization.

Syntax

```
[no] authorization {server-name | service-group service-group-name}
  [ldap-base-dn-from-cert]
  [ldap-search-filter filter-string]
```

Parameter	Description
server-name	Specifies the name of a previously configured ACOS LDAP authorization server.
service-group *service-group-name*	Specifies the name of a previously configured ACOS LDAP service group.
ldap-base-dn-from-cert	Specifies that LDAP authorization process uses the Subject DN as the LDAP search base DN.
ldap-search-filter *filter-string*	Provides the LDAP filter used in the authorization process. The syntax rules for this filter string are provided in RFC 4515.

Mode SLB client SSL template configuration mode

Example Configure an LDAP server for client SSL authorization:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# authorization ldap1 ldap-base-dn-from-cert
```

ca-cert

Description Specify the name of the Certificate Authority (CA) certificate to use for validating client certificates. The CA certificate must be installed on the ACOS device.

The ACOS device is configured at the factory with the CA certificate bundle file "default_ca_bundle," including common trusted certificate authorities. Use the **show pki ca-cert** command to view the list of ca-certificates.

Use the **import ca-cert** command to install the CA certificate. If either of the **ocsp** options is included in the command line, ACOS checks client's SSL certificate via OCSP CA rather than using the CRL of the CA-signer.

NOTE: Additionally, you can update the 'a10_autoupdate_ca' CA bundle file for shared partition from the GLM server using the **automatic-update** command.

Syntax

```
[no] ca-cert cert-name [partition shared]
[ocsp {ocsp-server-name | service-group ocsp-service-group-name}]
```

Parameter	Description
cert-name	CA certificate name (1-255 characters). You can also use the CA bundle 'a10_autoupdate_ca' name installed on the GLM server.
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.
ocsp-server-name	Name of the OCSP server.
ocsp-service-group-name	Name of the OCSP service group.

Default Disabled

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# ca-cert exampleCA ocsp ocsp-server1
```

certificate

Description Specifies the name of the certificate to use for terminating or initiating an SSL connection. The certificate must be installed on the ACOS device.

A second certificate can be assigned to a template by using the alternate option. Two certificates assigned to a template must be of different types (RSA, ECDSA). A major (first) certificate must be assigned before an alternate (second) certificate is accepted by the template.

NOTE: The certificate command is used to replace the old cert/cert-alternate/key/key-alternate/chain-cert command. The new certificate configuration cannot co-exist with these commands.

Syntax

```
[no] certificate <cert-name> key <key-name> [pass-phrase
<pass-phrase-str>] [chain-cert <chain-cert-name>] [partition
shared]
```

Parameter	Description
cert-name	Specifies the CA certificate name (1-245 characters).
key-name	Specifiesthe CA certificate key name (1-245 characters).
pass-phrase	Specifies the password phrase (1-128 characters).
chain-cert-name	Specifies a certificate-key chain. (1-245 characters).
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# certificate Cert123.pem key key123
pass-phrase Pass123
```

cipher

Description Specifies the cipher suite to support for certificates from clients.

Syntax

```
[no] cipher cipher-name
```

Parameter	Description
cipher-name	CA certificate name (1-255 characters). By default, all supported ciphers are enabled. The supported cipher are listed at axseries. You can remove (or re-add) one cipher in the template with a single command. Enter separate commands for each cipher to remove or re-add.

Mode SLB client SSL and server SSL template Configuration

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# cipher TLS1_ECDHE_RSA_AES_256_SHA384
```

client-certificate

Description Specifies the action that the ACOS device takes in response to a client's connection request.

Syntax

```
[no] client-certificate {Ignore | Require | Request}
```

Parameter	Description
Ignore	The ACOS device does not request the client to send its certificate.
Require	The ACOS device requires the client certificate. This action requests the client to send its certificate.

Parameter	Description
	However, the SSL handshake does not proceed (it fails) if the client sends a NULL certificate or the certificate is invalid.
Request	The ACOS device requests the client to send its certificate. With this action, the SSL handshake proceeds even if either of the following occurs: • The client sends a NULL certificate (one with zero length). • The certificate is invalid, causing client verification to fail. Use this option if you want the request to trigger an aFleX policy for further processing.

Default Ignore.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# client-certificate Require
```

client-certificate-Request-CA

Description Specifies the name of a CA certificate used in requests for client authentication.

Syntax

```
[no] client-certificate-Request-CA cert-name [partition shared]
```

Parameter	Description
cert-name	Specifies a second (or alternate) certificate (1-255 characters).
partition shared	Bind shared client-certificate-Request-CA in private partition's client-SSL template.

Default No default.

Mode SLB client SSL template configuration mode

Usage Multiple CA certificates can be configured as described in the following example.

Example The following commands configure the ACOS device to request the client certificate and to send the list of more than 10 CAs in the certificate request. This is achieved by configuring a chain cert (named LargeExample.chain below) that contains multiple CA certificates:

```
ACOS(config)#slb template client-ssl client-ssl-example-name
ACOS(config-client ssl)#client-certificate-Request-CA ca1.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca2.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca3.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca4.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca5.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca6.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca7.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca8.crt
ACOS(config-client ssl)#client-certificate-Request-CA ca9.crt
ACOS(config-client ssl)#client-certificate-Request-CA
LargeExample.chain
```

Example The following commands bing shared partition alternate certificate:

```
ACOS[partition1](config)#slb template client-ssl client-ssl-
example-shared
ACOS[partition1](config-client ssl)#client-certificate-
Request-CA ca1.crt partition shared
```

close-notify

Description Enables close notification (close_notify) alerts for SSL sessions.

Syntax

```
[no] close-notify
```

Default Disabled

Mode SLB client SSL template

Usage When this command is enabled, the ACOS device sends a close_notify message when an SSL transaction ends, before sending a FIN. This

behavior is required by certain types of client applications, including PHP cgi. For this type of client, if the ACOS device does not send a close_notify, an error or warning appears on the client.

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# close-notify
```

crl

Description Specifies a list of client certificates that have been revoked by the Certificate Authority (CA) that signed them. This option is applicable only if the ACOS device will be required to validate the identities of clients.

The CRL should be signed by the same issuer as the CA certificate. Otherwise, the client and ACOS device will not be able to establish a connection.

Syntax

```
[no] crl file-name [partition shared]
```

Parameter	Description
file-name	CRL file name (1-255 characters).
partition shared	Bind shared client-certificate-Request-CA in private partition's client-SSL template.

Mode SLB client SSL template configuration mode

Example Example configuration:

Example This example shows how to add CRL and CA certificates to a client-SSL template.

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# client-certificate Require
ACOS(config-client ssl)# crl 10_ca.crt_crl.pem
ACOS(config-client ssl)# crl 20_ca.crt_crl.pem
ACOS(config-client ssl)# crl root-ca.pem.crl.pem
ACOS(config-client ssl)# ca-cert 10_ca_crt
ACOS(config-client ssl)# ca-cert 20_ca.crt
```

```
ACOS(config-client ssl)# ca-cert root-ca.pem
```

NOTE: If you plan to use a CRL, you must set the **client-certificate** mode to **Require**.

dh-param

Description Specify Diffie-Hellman parameters.

Syntax

```
[no] dh-param {1024 | 1024-dsa | 2048}
```

Default Not enabled.

Mode SLB client SSL and server SSL template configuration mode

Example Example configuration for client SSL template:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# dh-param 1024
```

Example Example configuration for server SSL template:

```
ACOS(config)#  slb template server-ssl serverssl
ACOS(config-client ssl)# dh-param 1024
```

direct-client-server-auth

Description Allow the backend server to perform SSL client authentication directly.

Syntax

```
[no] direct-client-server-auth
```

Default Not enabled.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# direct-client-server-auth
```

disable-sslv3

Description Disables support for SSLv3 in client-SSL templates.

NOTE: If you disable SSLv3 support, when ACOS receives an SSL Hello message from a client, ACOS responds by sending a TCP-FIN to the client to end the session.

Syntax

```
[no] disable-sslv3
```

Default SSLv3 support is enabled by default.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# disable-sslv3
```

early-data

Description Enables the early data (0-RTT) for SSL version TLSv1.3.

Additionally, you must configure **session-cache-size** to do PSK resumption.

NOTE:
- Supported on new N5 module, QAT module, and Software TLS 1 .3.
- Maximum value is set to 16384 once enabled and is non-editable.

Syntax

```
[no] early-data [no-anti-replay]
```

Parameter	Description
early-data no-anti-replay,	Enable 0-RTT with no-anti-replay to prevent replay attack. Additionally, you must configure either **session-cache-size** or **session-ticket-enable** to do PSK resumption.

Default Not enabled.

Mode SLB client SSL template configuration mode

Usage This allows the TLS client to send encrypted data in the same packet as the Client Hello during the handshake for resumed sessions.

Example The following commands configure a cipher template:

```
ACOS(config)# slb template cipher cipther_tls_1.3
ACOS(config-cipher)# tls1_3 TLS_AES_256_GCM_SHA384
ACOS(config-cipher)# tls1_3 TLS_CHACHA20_POLY1305_SHA256
ACOS(config-cipher)# tls1_3 TLS_AES_128_GCM_SHA256
ACOS(config-cipher)# end
```

Example The following command binds the cipher template, `cipher_tls_1.3`, to the client-SSL template, `clnt-0rtt-test`:

```
ACOS(config)# slb template client-ssl clnt-0rtt-test
ACOS(config-client ssl)# ec-name secp384r1
ACOS(config-client ssl)# close-notify
ACOS(config-client ssl)# template cipher cipther_tls_1.3
ACOS(config-client ssl)# session-cache-size 50000
ACOS(config-client ssl)# version 34 33
ACOS(config-client ssl)# early-data
ACOS(config-client ssl)# certificate ecdhe-ecdsa.pem key
ecdhe-ecdsa.key
```

ec-name

Description Configures the Elliptic curve cryptographic (ECC) algorithm name for key exchange.

These algorithms use public or private key pairs, where the private key is an integer and the public key is a point on the elliptic curve (EC point).

Syntax

```
[no] ec-name {secp256r1 | secp384r1 | secp521r1 | x25519}
```

Parameter	Description
secp256r1	Specify the standard 256-bit cryptographic curve name.
secp384r1	Specify the standard 384-bit cryptographic curve name.
secp521r1	Specify the secured 521-bit cryptographic curve name.

Parameter	Description
	This option is supported only for the following SSL modules: • Intel QuickAssist Technology (QAT) SSL module with both TLS 1.2 and TLS 1.3 • Software SSL module TLS 1.2 and 1.3
x25519	Specify the secured 128 bits (256-bit key size) cryptographic curve name. This option is supported only for the following SSL modules: • Intel QuickAssist Technology (QAT) SSL module in both TLS 1.2 and TLS 1.3 • Software SSL module TLS 1.2 and 1.3

Default NA

Mode SLB client and server SSL template configuration mode

Usage All the ec-name options can be configured at the same time in the client and server SSL templates. The key exchange takes place based on the SSL module and SSL version configuration.

The following scenarios are considered for the key exchange negotiated between the client and server:

- ec-name is configured - ACOS checks whether the peer's supported groups are available in the ec-name configuration; if not, the key exchange fails. But if it is configured, the key exchange will succeed.
- ec-name is not configured - ACOS checks whether it supports the EC corresponding to peer's supported groups; if not, the key exchange fails.

Example Example configuration for Client SSL:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# ec-name secp521r1
ACOS(config-client ssl)# ec-name x25519
```

Example Example configuration for Server SSL:

```
ACOS(config)#  slb template server-ssl serverssl
ACOS(config-server ssl)# ec-name secp521r1
ACOS(config-server ssl)# ec-name x25519
```

Related Commands:

- version under client-SSL template
- version under server-SSL template

enable-ssli-ftp-alg

Description Enables FTP passive mode over TLS support for the specified port number. The port number value can between 1-65535.

NOTE: This configuration is applicable for implicit FTPS.

Syntax

```
[no] enable-ssli-ftp-alg port-num {<1-65535>}
```

Default Disabled.

Mode SLB client and server SSL template configuration mode

Example Example configuration for Client-SSL:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# enable-ssli-ftp-alg 990
```

Example Example configuration for Server-SSL:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-client ssl)# enable-ssli-ftp-alg 990
```

enable-tls-alert-logging fatal

Description Enables logging of TLS alerts that include the flow information such as source IP address.

Syntax

```
[no] enable-tls-alert-logging fatal
```

Default Disabled by default.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# enable-tls-alert-logging fatal
```

forward-proxy-alt-sign cert

Description Configure the forward proxy alternate signing certificate, certificate key, and chain cert. Optionally, sets a password phrase and bind a shared partition's certificate.

If the SSL site requested by the client is not on the trusted list (set by the `forward-proxy-trusted-ca` command), the inside ACOS device signs the cert with the key specified by this command.

Syntax

```
[no] forward-proxy-alt-sign cert <cert-name> key <key-name>
[pass-phrase
<pass-phrase>] [chain-cert <chain-cert-name>] [partition
shared]
```

Parameter	Description
cert-name	Specifies the certificate name (1-245 characters).
key-name	Specifies the certificate key name (1-245 characters).
pass-phrase	Specifies the password phrase (1-128 characters).
chain-cert-name	Specifies a certificate-key chain. (1-245 characters).
partition shared	Bind shared partition’s alternate certificate in private partition’s client-SSL template.

Mode SLB client SSL template configuration mode

Example Example configuration.

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-alt-sign cert
certificate Cert123.pem key key123 pass-phrase Pass123 chain-
cert exampleCA partition shared
```

forward-proxy-block-message

Description Sets a block message that is displayed on a webpage if a user encounters an invalid SSLi certificate issue.

Syntax

```
[no] forward-proxy-block-message custom_message
```

Parameter	Description
custom_message	A custom message. A string

Mode SLB client SSL template configuration mode

Example The following command configures a custom block message for a certificate revocation error.

```
ACOS(config-client ssl)# forward-proxy-cert-revoke-action
block
ACOS(config-client ssl)# forward-proxy-block-message "This
website cannot be displayed as there is a certificate issue."
```

forward-proxy-bypass ad-group-list

Description Bypasses SSLi inspection if AD group name matches a class list entry.

Syntax

```
[no] forward-proxy-bypass ad-group-list
```

Parameter	Description
ad-group-list	Name of the AD group list. A string.

Default None.

Mode SLB client SSL template configuration mode

Usage Use this command to bypass SSLi inspection by matching an AD group name in the group list name. The group list must already be configured.

Example The following example configures forward-proxy-bypass for all members of the AD group lisr USERS. The group list must be preconfigured:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)#forward-proxy-bypass ad-group-list
```

forward-proxy-bypass case-insensitive

Description Disables case sensitivity for string matching in SSLi bypass.

Syntax

```
[no] forward-proxy-bypass case-insensitive
```

Default By default, matching is case sensitive.

Mode SLB client SSL template configuration mode

Usage Use this command to disable case sensitivity for matching strings in SSLi bypass.

For example, the **forward-proxy-bypass** contains aa rule searches for matches on SNI strings that contain "aa" but not on strings that contain "AA". You can also enable or disable case-sensitive matching. In this case, the rule shown above matches SNI strings that contain any of the following: "aa", "AA", "aA", or "Aa". You can disable case sensitivity on a template-wide basis. The setting applies to all match rules in the template.

Additionally, the behavior of **forward-proxy-bypass case-insensitive** configuration is as follows:

- In the below example, the case-insensitive match is performed as the matching rule is configured directly.

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-bypass case-insensitive
ACOS(config-client ssl)# forward-proxy-bypass contains
a10networks.com
```

- In the below example, the case-sensitive match is performed as the matching rule is configured with a class list. The **forward-proxy-bypass case-insensitive** configuration has no effect in this scenario.

```
ACOS(config)# class-list mylist
ACOS(config-class list)# contains a10networks.com
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-bypass case-insensitive
ACOS(config-client ssl)# forward-proxy-bypass class-list
mylist
```

This behavior is also applicable to forward-proxy-bypass client-auth **case-insensitive** option.

Example The following example configures forward-proxy-bypass as case-insensitive for all matches in the client-ssl template:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-bypass case-insensitive
ACOS(config-client ssl)# forward-proxy-bypass contains aa
```

forward-proxy-bypass central-cert-pin-list

Description Configures the SSLi intercept decision-making for central cert pinning list.

NOTE: If both central and local cert pinning list are set in the client-ssl template, the central cert pinning list takes precedence.

Syntax

```
[no] forward-proxy-bypass central-cert-pin-list
```

Default Disabled

Mode SLB client SSL template

Usage The following process describes the SSLi bypass decision mechanism:

1. The bypass filter is invoked when Thunder receives a request, and the client SSL bypass/exception-bypass rule is configured.
2. Once the centrally generated cert-pinning-candidate-list bypass rule is set, the bypass filter will look first at this list.
3. If SNI string is in the central cert pinning list then the bypassed rule is matched and the process will continue to bypass.
4. If not, it will check the other bypass and exception rules in the correct order.
5. If none of the rules are met, the intercept procedure will be initiated.

Example The following example configures the bypass rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass central-cert-pin-list
```

Related Commands:

- cert-pinning
- forward-proxy-bypass local-cert-pin-list

forward-proxy-bypass certificate-issuer

Description Configures SSLi bypass based on the string from a certificate issuer.

Syntax

```
[no] forward-proxy-bypass certificate issuer { class-list { class_list_name | multi-class-list multi_class_list_name } | contains certificate_issuer_name | ends-with certificate_issuer_name | equals certificate_issuer_name | exception-class-list exceptionclass-list_name | starts-with certificate_issuer_name }
```

Parameter	Description
certificate_issuer_name	Name of the certificate issuer. A string.
class-list	Bypasses SSLi if the certificate issuer matches the class-list. When enabled, the **multi-class-list** command option allows you to enter up to 16 file-type class lists for each **slb template client-ssl** instance. If not enabled by the **multi-class-list** command option, you can enter only one class list name.
contains	Bypasses SSLi if certificate issuer contains a string that matches the configured string.
ends-with	Bypasses SSLi if certificate issuer ends with a string that matches the configured string.
equals	Bypasses SSLi if certificate issuer equals a string that matches the configured string.
exception-class-list	Exception class-list to forward-proxy-bypass.
starts-with	Bypasses SSLi if certificate issuer starts with a string that matches the configured string.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi bypass based on certificate issuer. To determine the Certificate Authority that issued your certificate, open the website in a browser and click on the certificate information.

The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for bypassing SSLi if the certificate-issuer contains the string **Norton**:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-bypass certificate-
issuer
contains Norton
```

forward-proxy-bypass certificate-san

Description Configures SSLi bypass based on the string from a certificate SAN.

Syntax

```
[no] forward-proxy-bypass certificate-san { class-list {
class_list_name | multi-class-list multi_class_list_name } |
contains certificate_san_name | ends-with certificate_san_name
| equals certificate_san_name | exception-class-list
exceptionclass-list_name | starts-with certificate_san_name }
```

Parameter	Description
certificate_san_name	Name of the certificate SAN. A string.
class-list	Bypasses SSLi if the certificate SAN matches the class-list. When enabled, the **multi-class-list** command option allows you to enter up to 16 file-type class lists for each **slb template client-ssl** instance. If not enabled by the **multi-class-list** command option, you can enter only one class list name.
contains	Bypasses SSLi if certificate SAN contains a string that matches the configured string.
ends-with	Bypasses SSLi if certificate SAN ends with a string that matches the configured string.
equals	Bypasses SSLi if certificate SAN equals a string that matches the configured string.
exception-class-list	Exception class-list to forward-proxy-bypass.
starts-with	Bypasses SSLi if certificate SAN starts with a string that matches the configured string.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi bypass based on certificate SAN. Subject Alternative Name (SAN) certificates can secure a number of fully qualified domain names with a single certificate. The SAN field enables you to specify additional host names such as sites, IP addresses, common names, and so on, to be protected by a single SSL Certificate.

The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.

- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for bypassing SSLi if the certificate-SAN contains the string **a10**:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-bypass certificate-san
contains a10
```

forward-proxy-bypass certificate-subject

Description Configures SSLi bypass based on the string from a certificate subject.

Syntax

```
[no] forward-proxy-bypass certificate-subject { class-list {
class_list_name | multi-class-list multi_class_list_name } |
contains certificate_sub_name | ends-with certificate_sub_name
| equals certificate_sub_name | exception-class-list
exceptionclass-list_name | starts-with certificate_sub_name }
```

Parameter	Description
certificate_ sub_name	Name of the certificate subject. A string.
class-list	Bypasses SSLi if the certificate subject matches the class-list. When enabled, the **multi-class-list** command option allows you to enter up to 16 file-type class lists for each **slb template client-ssl** instance. If not enabled by the **multi-class-list** command option, you can enter only one class list name.
contains	Bypasses SSLi if certificate subject contains a string

Parameter	Description
	that matches the configured string.
ends-with	Bypasses SSLi if certificate subject ends with a string that matches the configured string.
equals	Bypasses SSLi if certificate subject equals a string that matches the configured string.
exception-class-list	Exception class-list to forward-proxy-bypass.
starts-with	Bypasses SSLi if certificate subject starts with a string that matches the configured string.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi bypass based on certificate subject. The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for bypassing SSLi if the certificate-subject contains the string **a10**:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-bypass certificate-subject contains a10
```

forward-proxy-bypass class-list

Description Configures SSLi bypass when the SNI of the outside server matches based on the specified class list or class-lists.

Syntax

```
[no] forward-proxy-bypass class-list { class_list_name |
multi-class-list multi_class_list_name }
```

Parameter	Description
class-list *class_list_name*	Name of the class-list.
multi-class-list *multi_class_list_name*	Name of the multi-class-list. When enabled, the **multi-class-list** command option allows you to enter up to 16 file-type class lists for each **slb template client-ssl** instance. If not enabled by the **multi-class-list** command option, you can enter only one class list name.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi bypass when the SNI of the outside server matches based on the specified class list or class-lists. The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals,

starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for bypassing SSLi if the SNI of the outside server matches any entry in two multiple-class-lists:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass class-list
multi-class-list my-classlist-name1
ACOS(config-client ssl)# forward-proxy-bypass class-list
multi-class-list my-classlist-name2
```

forward-proxy-bypass client-auth

Description Configures the SNI attributes and/or class-lists that determine whether or not a client is enabled for client-authentication SSLi bypass. These attributes and class-lists are bound to an SSL client template which itself is bound to the ACOS decrypt device.

Syntax

```
[no] forward-proxy-bypass client-auth { case-insensitive |
class-list { class_list_name | multi-class-list multi_class_
list_name } | contains sni_string | ends-with sni_string |
equals sni_string | starts-with sni_string }
```

Parameter	Description
case-insensitive	See forward-proxy-bypass case-insensitive for more information.
class-list	Bypasses SSLi if the SNI attributes matches the class-list. When enabled, the **multi-class-list** command option allows you to enter up to 16 file-type class lists for each **slb template client-ssl** instance. If not enabled by the **multi-class-list** command option, you can enter only one class list name.
contains	Bypasses SSLi if the SNI attributes contains a string that matches the configured string.
ends-with	Bypasses SSLi if the SNI attributes ends with a string that matches the configured string.

Parameter	Description
`equals`	Bypasses SSLi if the SNI attributes equals a string that matches the configured string.
`starts-with`	Bypasses SSLi if the SNI attributes starts with a string that matches the configured string.

Default None

Mode SLB client SSL template configuration mode

Usage Some HTTPS servers might require client certificate authentication (CAC/PKI) when the server authenticates incoming requests based on the certificate in the client's certificate store. The ACOS decrypt device detects whether the remote server requires client certificate authentication. If the server requires client authentication, the ACOS device checks whether the the configuration matches a condition to bypass this traffic. If a match is found, ACOS_decrypt stops SSLi processing and switches from HTTPS processing to basic TCP proxy processing.

The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures three conditions for client-authentication bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass client-auth
class-list testclass
ACOS(config-client ssl)# forward-proxy-bypass client-auth
contains jsmith
ACOS(config-client ssl)# forward-proxy-bypass client-auth
equals test.hello.com
```

forward-proxy-bypass client-ip-list

Description Configures bypass rule if the client IP matches the class-list.

Syntax

```
[no] forward-proxy-bypass client-ip-list {ipv4 class-list-name
| ipv6 class-list-name}
```

Parameter	Description
ipv4/ipv6 *class-list-name*	Specify the IPv4 or IPv6 client class-list name to be bound with the client-SSL template. The value can be between 1-63. **NOTE:** You can also configure multiple class-list (up to 8) of each IPv4 or IPv6 type.

Default None

Mode SLB client SSL template configuration mode

Usage When the client IP belongs to any one of the configured class-lists, the request will be bypassed.

Additionally, the following bypass filter shall be considered for SSLi bypass decision-making:

- The bypass filter will first check the 'client-ip-list' and then 'server-ip-list', if both the options are configured.
- The bypass filter will first check the 'exception-ip-list' and then 'ip-list', if both the options are configured.

Example The following example configures a client class-list for IPv4:

```
ACOS(config)#class-list class-list_ipv4 ipv4
```

```
ACOS(config-class list)#1.1.1.0/24
```

The following example binds a client class-list to the client-ssl template for bypass rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass client-ip-list
ipv4 class-list_ipv4
```

Example The following example configures the multiple client class-list for IPv4:

```
ACOS(config)#class-list C1 ipv4
ACOS(config-class list)#1.1.1.0/24
ACOS(config-class list)#class-list C2 ipv4
ACOS(config-class list)#1.1.1.1/24
ACOS(config-class list)#class-list C3 ipv4
ACOS(config-class list)#1.1.1.2/24
```

The following example binds the multiple client class-list to the client-ssl template for bypass rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass client-ip-list
ipv4 C1
ACOS(config-client ssl)#forward-proxy-bypass client-ip-list
ipv4 C2
ACOS(config-client ssl)#forward-proxy-bypass client-ip-list
ipv4 C3
```

Related Commands:

- forward-proxy-bypass server-ip-list
- forward-proxy-bypass exception-client-ip-list
- forward-proxy-bypass exception-server-ip-list

forward-proxy-bypass contains

Description Configures SSLi bypass if SNI string contains the configured string.

Syntax

```
[no] forward-proxy-bypass contains sni_string
```

Parameter	Description
sni_string	Name of the SNI.

Default None

Mode SLB client SSL template configuration mode

Usage The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for SSLi bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass contains A10
```

forward-proxy-bypass ends-with

Description Configures SSLi bypass if SNI string ends with the configured string.

Syntax `[no] forward-proxy-bypass ends-with sni_string`

Parameter	Description
sni_string	Name of the SNI.

Default None

Mode SLB client SSL template configuration mode

Usage The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for SSLi bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass ends-with A10
```

forward-proxy-bypass equals

Description Configures SSLi bypass if SNI string equals the configured string.

Syntax

```
[no] forward-proxy-bypass equals sni_string
```

Parameter	Description
sni_string	Name of the SNI.

Default None

Mode SLB client SSL template configuration mode

Usage The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.

- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for SSLi bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass equals A10
```

forward-proxy-bypass exception-ad-group-list

Description Configures exceptions to SSLi bypass if AD group name matches an entry in the exception AD group list.

Syntax

```
[no] forward-proxy-bypass exception-ad-group-list
exception_ad_group_list_name
```

Parameter	Description
exception_ad_group_list_name	Name of the exception AD group list.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to configure exceptions for SSLi bypass.

Example The following example configures an exception class list for exceptions for SSLi bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass exception-
class-list mylist
```

forward-proxy-bypass exception-class-list

Description Configures exceptions to SSLi bypass if SNI string matches an entry in the exception class list.

Syntax

```
[no] forward-proxy-bypass exception-class-list
exception_class_list_name
```

Parameter	Description
exception_class_list_name	Name of the exception class list.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to configure exceptions for SSLi bypass.

Example The following example configures an exception class list for exceptions for SSLi bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass exception-
class-list mylist
```

forward-proxy-bypass exception-client-ip-list

Description Configures intercept rule if the client IP matches the class-list.

Syntax

```
[no] forward-proxy-bypass exception-client-ip-list {ipv4
class-list-name | ipv6 class-list-name}
```

Parameter	Description
ipv4/ipv6 *class-list-name*	Specify the IPv4 or IPv6 client class-list name to be bound with the client-SSL template. The value can be between 1-63. You can also configure multiple class-list (up to 8) of each IPv4/IPv6 type.

Default None

Mode SLB client SSL template configuration mode

Usage When the client IP belongs to any one of the configured class-lists, the request will be intercepted.

Additionally, the following bypass filter shall be considered for SSLi bypass or intercept decision-making:

- The bypass filter will first check the 'exception-ip-list' and then 'ip-list', if both the options are configured.
- The bypass filter will first check the 'exception-client-ip-list' and then 'exception-server-ip-list', if both the options are configured.

Example The following example configures a client class-list for IPv4:

```
ACOS(config)#class-list class-list_ipv4 ipv4
ACOS(config-class list)#1.0.3.4/24
```

The following example binds a client class-list to the client-ssl template for intercept rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass exception-client-ip-list ipv4 class-list_ipv4
```

Example The following example configures the multiple client class-list for IPv4:

```
ACOS(config)#class-list C1 ipv4
ACOS(config-class list)#1.1.1.0/24
ACOS(config-class list)#class-list C2 ipv4
ACOS(config-class list)#1.1.1.1/24
ACOS(config-class list)#class-list C3 ipv4
ACOS(config-class list)#1.1.1.2/24
```

The following example binds the multiple client class-list to the client-ssl template for intercept rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass exception-client-ip-list ipv4 C1
ACOS(config-client ssl)#forward-proxy-bypass exception-client-ip-list ipv4 C2
ACOS(config-client ssl)#forward-proxy-bypass exception-client-ip-list ipv4 C3
```

Related Commands:

- forward-proxy-bypass exception-server-ip-list
- forward-proxy-bypass client-ip-list
- forward-proxy-bypass server-ip-list

forward-proxy-bypass exception-server-ip-list

Description Configures intercept rule if the server IP matches the class-list.

Syntax

```
[no] forward-proxy-bypass exception-server-ip-list {ipv4 class-list-name | ipv6 class-list-name}
```

Parameter	Description
ipv4*class-list-name*	Specify the IPv4 server class-list name to be bound with the client-SSL template. The value can be between 1-63. You can also configure multiple class-list (up to 8) of each IPv4 type.
ipv6 *class-list-name*	Specify the IPv6 server class-list name to be bound with the client-SSL template. The value can be between 1-63. You can also configure multiple class-list (up to 8) of each IPv6 type.

Default None

Mode SLB client SSL template configuration mode

Usage When the server IP belongs to any one of the configured class-lists, the request will be intercepted.

Additionally, the following bypass filter shall be considered for SSLi bypass or intercept decision-making:

- The bypass filter will first check the 'exception-ip-list' and then 'ip-list', if both the options are configured.
- The bypass filter will first check the 'exception-client-ip-list' and then 'exception-server-ip-list', if both the options are configured.

Example The following example configures a server class-list for IPv4:

```
ACOS(config)#class-list class-list_ipv4 ipv4
ACOS(config-class list)#2.3.3.0/24
```

The following example binds a server class-list to the client-ssl template for intercept rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass exception-server-ip-list ipv4 class-list_ipv4
```

Example The following example configures the multiple server class-list for IPv4:

```
ACOS(config)#class-list S1 ipv4
ACOS(config-class list)#2.1.1.0/24
ACOS(config-class list)#class-list S2 ipv4
ACOS(config-class list)#2.1.1.1/24
ACOS(config-class list)#class-list S3 ipv4
ACOS(config-class list)#2.1.1.2/24
```

The following example binds the multiple server class-list to the client-ssl template for intercept rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass exception-server-ip-list ipv4 S1
ACOS(config-client ssl)#forward-proxy-bypass exception-server-ip-list ipv4 S2
ACOS(config-client ssl)#forward-proxy-bypass exception-server-ip-list ipv4 S3
```

Related Commands:

- forward-proxy-bypass exception-client-ip-list
- forward-proxy-bypass client-ip-list
- forward-proxy-bypass server-ip-list

forward-proxy-bypass exception-user-name-list

Description Configures an exception to SSLi bypass if a user name matches an entry in the user name exception class list.

Syntax

```
[no] forward-proxy-bypass exception-user-name-list exception_user_list_name
```

Parameter	Description
exception_user_list_name	Name of the exception user name list.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to configure exceptions for SSLi bypass based on user names.

Example The following example configures an exception user name list of **mylist**:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass exception-user-name-list mylist
```

forward-proxy-bypass exception-web-category

Description Configures SSLi intercept decision making based on web URL category.

Syntax

```
[no] forward-proxy-bypass exception-web-category web-category-name
```

Default None

Mode SLB client SSL template configuration mode

Usage ACOS connects with third-party servers (specifically, Webroot's BrightCloud servers), to obtain web-category for enhanced protection. To access theseservers, a URL Classification license is required.
When the web category matches the setting exception category list, the request would be intercepted.

NOTE: A client-ssl template can have multi entries of exception-web-category at a time, like web-category.

Example The following example configures web category exception for sports URLs:

```
ACOS(config)# slb template client-ssl SSL_webcategoryexception
ACOS-(config-client ssl)# forward-proxy-bypass exception-web-category sports
```

forward-proxy-bypass exception-web-reputation

Description Configures SSLi intercept decision making based on web URL reputation scope.

Syntax

```
[no] forward-proxy-bypass exception-web-reputation{reputation-scope}
```

Parameter	Description
trustworthy	To intercept URLs scores under 100. These are clean URLs and do no impose security risk.
low-risk	To intercept URLs scores under 80. These are benign URLs and exhibit very low security risk.
moderate-risk	To intercept URLs scores under 60. These are benign URLs and exhibit potential security risk.
suspicious	To intercept URLs scores under 40. These are suspicious URLs and exhibit predictive security risk.
malicious	To intercept URLs scores under 20. These are high risk URLs and exhibit high security risk.
<1-100>	To intercept URLs scores under the customized value (1-100).

Default None

Mode SLB client SSL template configuration mode

Usage When the web-reputation score is less than or equal to the level set or customized score, the request would be intercepted. Otherwise, SSLi will check other bypass criteria, and then make the decision. However, it does not bypass immediately.

NOTE: A client-ssl template can only have one entry of the exception-web-reputation at a time.

Example The following example configures web reputation exception for malicious URLs:

```
ACOS(config)# slb template client-ssl SSL_
webreputationexception
ACOS-(config-client ssl)# forward-proxy-bypass exception-web-
reputation malicious
```

forward-proxy-bypass local-cert-pin-list

Description Configures the SSLi intercept decision-making for the local cert pinning list.

Syntax

```
[no] forward-proxy-bypass local-cert-pin-list {conn-fail-
count}1-65536
```

Parameter	Description
conn-fail-count	Specify the connection fail count as the bypass criteria. The value can be between 1-65536. When the connection failure count exceeds the set criteria, the request would be bypassed. Also, the corresponding bypassed counter will increase and the TTL will be refreshed to the default or set value. For the bypassed cases, the connection-fail counter will not increase.

Default None

Mode SLB client SSL template configuration mode

Usage The following process describes the SSLi bypass decision mechanism:

1. The bypass filter is invoked when Thunder receives a request, and the client SSL bypass/exception-bypass rule is configured.
2. Once the local cert pinning list bypass rule is set, the bypass filter will first look at this list.
3. If the SNI string is in the local cert pinning list, and if the connection failure count exceeds the threshold defined in the rule, the decision process will be broken. However, the processes will continue to bypass.
4. If not, it will check the other bypass and exception rules in the correct order.

5. If none of the rules are met, the intercept procedure will be initiated.

Example The following example configures the bypass rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)# forward-proxy-bypass local-cert-pin-list conn-fail-count 100
```

Related Commands:

- cert-pinning
- forward-proxy-bypass central-cert-pin-list

forward-proxy-bypass require-web-category

Description Enables Web Category Lookup Enforcement for both the web-category and web-reputation based SSLi bypass policies under that template.

Web category lookup enforcement resolves the category and reputation of the unknown (first request) URLs by pausing the data plane connection. When the result is known and the URL is categorized or reputed, the connection is resumed.

Syntax

```
[no] forward-proxy-bypass require-web-category
```

Default Disabled

Mode SLB client SSL template configuration mode

Example The following example enables Web Category Lookup Enforcement for web-category based SSLi bypass policies under the BLUE client-ssl template.

```
ACOS(config)# slb template client-ssl BLUE
ACOS(config-client ssl)# forward-proxy-bypass web-category financial-services
ACOS(config-client ssl)# forward-proxy-bypass web-category health-and-medicine
ACOS(config-client ssl)# forward-proxy-bypass require-web-category
```

Example The following example enables Web Category Lookup Enforcement for web-reputation based SSLi bypass policies under the BLUE client-ssl template.

```
ACOS(config)# slb template client-ssl BLUE
ACOS(config-client ssl)# forward-proxy-bypass web-reputation financial-services
ACOS(config-client ssl)# forward-proxy-bypass require-web-category
```

forward-proxy-bypass starts-with

Description Configures SSLi bypass if the SNI string starts with the configured string.

Syntax

```
[no] forward-proxy-bypass starts-with sni_string
```

Parameter	Description
sni_string	Name of the SNI.

Default None

Mode SLB client SSL template configuration mode

Usage The following match options are used by the rules that you configure:

- Equals—Matches only if the value completely matches the specified string.
- Starts-with—Matches only if the value starts with the specified string.
- Contains—Matches if the specified string appears anywhere within the value.
- Ends-with—Matches only if the value ends with the specified string.

These match options are always applied in the order shown, regardless of the order in which the rules appear in the configuration. If a template has more than one rule with the same match option (equals, starts-with, contains, or ends-with) and a value matches on more than one of them, the most-specific match is always used.

Example The following example configures a condition for SSLi bypass:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass starts-with A10
```

forward-proxy-bypass server-ip-list

Description Configures bypass rule if the server IP matches the class-list.

Syntax

```
[no] forward-proxy-bypass server-ip-list {ipv4 class-list-name
| ipv6 class-list-name}
```

Parameter	Description
ipv4*class-list-name*	Specify the IPv4 server class-list name to be bound with the client-SSL template. The value can be between 1-63. You can also configure multiple class-list (up to 8) of each IPv4 type.
ipv6 *class-list-name*	Specify the IPv6 server class-list name to be bound with the client-SSL template. The value can be between 1-63. You can also configure multiple class-list (up to 8) of each IPv6 type.

Default None

Mode SLB client SSL template configuration mode

Usage When the server IP belongs to any one of the configured class-lists, the request will be bypassed.

Additionally, the following bypass filter shall be considered for SSLi bypass decision-making:

- The bypass filter will first check the 'client-ip-list' and then 'server-ip-list', if both the options are configured.
- The bypass filter will first check the 'exception-ip-list' and then 'ip-list', if both the options are configured.

Example The following example configures a server class-list for IPv4:

```
ACOS(config)#class-list class-list_ipv4 ipv4
ACOS(config-class list)#2.2.2.0/24
```

The following example binds a server class-list to the client-ssl template for bypass rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass server-ip-list
ipv4 class-list_ipv4
```

Example The following example configures multiple server class-list for IPv4:

```
ACOS(config)#class-list S1 ipv4
ACOS(config-class list)#1.1.1.0/24
ACOS(config-class list)#class-list S2 ipv4
ACOS(config-class list)#1.1.1.1/24
ACOS(config-class list)#class-list S3 ipv4
ACOS(config-class list)#1.1.1.2/24
```

The following example binds the multiple server class-list to the client-ssl template for bypass rule:

```
ACOS(config)#slb template client-ssl SSL_Client
ACOS(config-client ssl)#forward-proxy-bypass server-ip-list
ipv4 S1
ACOS(config-client ssl)#forward-proxy-bypass server-ip-list
ipv4 S2
ACOS(config-client ssl)#forward-proxy-bypass server-ip-list
ipv4 S3
```

Related Commands:

- forward-proxy-bypass client-ip-list
- forward-proxy-bypass exception-client-ip-list
- forward-proxy-bypass exception-server-ip-list

forward-proxy-bypass web-category

Description Configures SSLi bypass based on URL Classification. When URLs are categorized, this information can be used to filter out unwanted content to add an additional layer of security, or it can be used to

determine which URLs should bypass SSLi decryption in compliance with privacy laws.

For more information on the web-category-name refer web-category.

Syntax `[no] forward-proxy-bypass web-category web-category-name`

Default None

Mode SLB client SSL template configuration mode

Usage ACOS connects with third-party servers (specifically, Webroot's BrightCloud servers), to obtain web-category for enhanced protection. To access these servers, a URL Classification license is required.

Example The following example configures SSLi bypass for websites related to sports and real-estate:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass web-category
sports
ACOS-(config-client ssl)# forward-proxy-bypass web-category
real-estate
```

Example The following example configures SSLi bypass for websites related to child abuse material (CAM):

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass web-category
illegal-pornography
ACOS-(config-client ssl)# forward-proxy-bypass web-category
nudity-artistic
```

forward-proxy-bypass web-reputation

Description Configures SSLi bypass decision making based on web URL reputation scope.

Syntax `[no] forward-proxy-bypass web-reputation {reputation-scope}`

Parameter	Description
trustworthy	To bypass URLs scores above 81. These are clean

Parameter	Description
	URLs and do no impose security risk.
low-risk	To bypass URLs scores above 61. These are benign URLs and exhibit very low security risk.
moderate-risk	To bypass URLs scores above 41. These are benign URLs and exhibit potential security risk.
suspicious	To bypass URLs scores above 21. These are suspicious URLs and exhibit predictive security risk.
malicious	To bypass URLs scores above 1. These are high risk URLs and exhibit high security risk.
<1-100>	To bypass URLs scores above the customized value (1-100).

Default None

Mode SLB client SSL template configuration mode

Usage When the web-reputation score is greater than or equal to the level set or customized score, the request would be bypassed. Otherwise, SSLi will check other intercept criteria, and then make the decision. However, it does not intercept immediately.

NOTE: A client-ssl template can only have one entry of web-reputation at a time.

Example The following example configures web reputation for trustworthy URLs:

```
ACOS(config)# slb template client-ssl SSL_webreputation
ACOS-(config-client ssl)# forward-proxy-bypass web-reputation trustworthy
```

forward-proxy-ca-certificate

Description Configure the forward proxy CA-signed certificate, certificate key, and chain cert. Optionally, sets a password phrase and bind a shared partition's certificate.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in the SSLi configurations.

Syntax

```
[no] forward-proxy-ca-certificate<cert-name> key <key-name>
[pass-phrase
<pass-phrase>] [chain-cert <chain-cert-name>] [partition
shared]
```

Parameter	Description
cert-name	Specifies the certificate name (1-245 characters).
key-name	Specifies the certificate key name (1-245 characters).
pass-phrase	Specifies the password phrase (1-128 characters).
chain-cert-name	Specifies a certificate-key chain. (1-245 characters).
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-ca-certificate
Cert123.pem key key123 pass-phrase Pass123 chain-cert myCAcert
```

forward-proxy-cache-persistence

Description Specifies an Aho-Corasick (AC) class-list of SNIs of forged certificates that are to be retained in the cache when ACOS is rebooted or whenever the ACOS forward-proxy process is restarted. If an SNI in the certificate matches an entry in this class list, it is retained; otherwise, it is dropped.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax

```
[no] forward-proxy-cache-persistence class-list name
```

Parameter	Description
name	Class-list name (1-63 characters).

Default If a persist class list is not bound to a client-SSL template, the cached forged certificates do not persist.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cache-persistence
class-list cl1
```

forward-proxy-cert-cache

Description Configures forward proxy certificate cache options.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax `[no] forward-proxy-cert-cache {limit bytes | timeout seconds}`

Parameter	Description
limit	Specifies the certificate cache size limit in bytes (0-2147483647). The default is 524288. Set the limit to 0 for unlimited size.
timeout	Specifies the certificate cache timeout value in seconds (0-2147483647). The default is 1 hour. Set the timeout to 0 for the certificate cache to never timeout. A Certificate can remain in the cache up to the value set in cache timeout. When a certificate exceeds that time, it is removed.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cert-cache timeout 7200
```

forward-proxy-cert-expiry

Description The number of hours that the forward proxy certificates will be valid.

Shortening the lifetime of the forged forward-proxy certs reduces the security risk if any are stolen. From 1 to 168 hours can be specified.

If the expiry occurs after the validity end-date, then this command will adjust the validity end date.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax

```
[no] forward-proxy-cert-expiry hours hours
```

Parameter	Description
hours	Number of hours (1-168).

Default By default, the forged forward proxy certs have the same expiration as the original certificates.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cert-expiry hours 48
```

forward-proxy-cert-ext

Description Specify the certificate extension for a Certificate Revocation List Distribution Point (CRLDP) or an Authority Information Access extension for Online Certificate Status Protocol (OCSP) or Certificate Authority (CA) Issuer for certificate validation.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax

```
[no] forward-proxy-cert-ext {crldp | aia {ca-issuers | ocsp}}
URI
```

Mode SLB client SSL template configuration mode

Example Example configuration to add a distribution point extension for a CRL.

```
ACOS(config)#slb template client-ssl SSL-Client
ACOS(config-client ssl)#forward-proxy-cert-ext crldp
http://www.example.com/example.crt
```

forward-proxy-cert-not-ready-action

Description Configures the action of the client connection if ACOS does not have the proxied cert ready.

Syntax

```
[no] forward-proxy-cert-not-ready-action {intercept | bypass |
reset}
```

- **bypass** - ACOS bypasses SSL proxy services and forwards the client packets to the actual SSL server.
- **reset** - ACOS requests an SSL connection reset. If the proxied cert is ready after the reset, the SSL proxy session is negotiated.
- **intercept** - ACOS intercepts SSL proxy services.

Default By default, SSL proxy session is bypassed when the proxied cert is not ready.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cert-not-ready-action
reset
```

forward-proxy-cert-revoke-action

Description Configures the action of the client connection if OCSP or CRL verification determines the certificate is irreversibly revoked.

Syntax

```
[no] forward-proxy-cert-revoke-action {bypass | continue |
drop
| block }
```

Parameter	Description
bypass	Bypasses the connection.
continue	Continues the connection.
drop	Drops the connection.
block	Blocks the connection. Use the **forward-proxy-block-message** command to draft a custom message to display when the connection is blocked.

Default By default, SSL proxy is bypassed if OCSP or CRL verification determines any certificate in the chain is unknown.

Mode SLB client SSL template configuration mode

Usage This command applies only to the certificates that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations. The options available are bypassing SSL Proxy, continuing with the connection, dropping the connection, or blocking the connection with a customizable mesage to the user.

Example The following example configures an SSLi connection as continued after a certificate revocation.

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cert-revoke-action
continue
```

Example The following example configures an SSLi connection as blocked and dispalys a custom blocked message:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cert-revoke-action
block
ACOS(config-client ssl)# forward-proxy-block-message "This
website cannot be displayed as there is a certificate issue."
```

forward-proxy-cert-unknown-action

Description Configures the action of the client connection if OCSP or CRL verification determines the certificate status is 'unknown.'

Syntax

```
[no] forward-proxy-cert-unknown-action {bypass | continue |
drop
| block }
```

Parameter	Description
bypass	Bypasses the connection.
continue	Continues the connection.
drop	Drops the connection.
block	Blocks the connection. Use the **forward-proxy-block-message** command to draft a custom message to display when the connection is blocked.

Default By default, SSL proxy is bypassed if OCSP or CRL verification determines any certificate in the chain is irreversibly revoked.

Mode SLB client SSL template configuration mode

Usage This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations. The options available are bypassing SSL Proxy, continuing with the connection, or dropping the connection.

Example The following example configures an SSLi connection as dropped after a certificate unknown error:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-cert-unknown-action
drop
```

Example The following example configures an SSLi connection as blocked and dispalys a custom blocked message:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# orward-proxy-cert-unknown-action
block
```

Example

```
ACOS(config-client ssl)# forward-proxy-block-message "This
website cannot be displayed as there is a certificate issue."
```

forward-proxy-cert-validity

Description Specify the starting and ending certificate validation period in which the certificate status and information will be maintained.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax

```
[no] forward-proxy-cert-validity {notafter | notbefore} day month year
```

Parameter	Description
day	Set the day of the month (1-31).
month	Set the month (1-12).
year	Set the year (2005-2035).

Default None.

Mode SLB Client SSL Template Configuration Mode

Example The following example shows how to add the starting validation time of November 1, 2005 for proxied certificates from the ACOS device.

```
ACOS(config)#slb template client-ssl SSL-Client
ACOS(config-client ssl)#forward-proxy-cert-validity notbefore
1 11 2005
```

forward-proxy-crl-disable

Description Disable Certificate Revocation List (CRL) services for SSLi (forward-proxy).

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax

```
[no] forward-proxy-crl-disable
```

Default By default, CRL for SSLi is enabled.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-crl-disable
```

forward-proxy-decrypted

Description Sets DSCP value for decrypted and bypassed traffic for SSLi configurations.

Syntax

```
[no] forward-proxy-decrypted dscp dscp_value_decrypted
dscp_value_bypassed
```

Parameter	Description
dscp_value_decrypted	DSCP value for decrypted traffic. The value ranges from 1 to 63.
dscp_value_bypassed	DSCP value for bypassed traffic. The value ranges from 1 to 63.

Default None.

Mode SLB client SSL template configuration mode

Usage Use this command to set the DSCP value for encrypted and bypassed traffic in an SSLi client template. If the service group has a template with DSCP configured, this command takes precedence.

Example Example configuration:

```
ACOS(config)# slb template client-ssl SSLi
ACOS(config-client ssl)# forward-proxy-decrypted dscp 6 1
```

forward-proxy-enable

Description Enables SSH Insight (SSHi) support on ACOS SLB virtual server.

Syntax

```
[no] forward-proxy-enable
```

Mode SLB client SSH template configuration mode

Example Example configuration:

```
ACOS-Inside(config)#slb template client-ssh SSHInsight_
ClientSide
```

```
ACOS-Inside(config client-ssh)#forward-proxy-hostkey RSA_key_
1234
ACOS-Inside(config-client-ssh)#forward-proxy-enable
```

forward-proxy-esni-action

Description Specify the action taken if the encrypted server name indication (ESNI) is recieved in ClientHello extension.

This command applies only to SSLi configurations.

Syntax

```
[no] forward-proxy-esni-action {drop | bypass }
```

Parameter	Description
bypass	Bypasses the connection.
drop	Drops the connection.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-esni-action drop
```

forward-proxy-failsafe-disable

Description Forward proxy (SSLi) failsafe enables SSLi traffic interception to be bypassed when there is a handshake failure. The most common handshake failures are due to servers only accepting elliptical ciphers.

This command applies only to SSLi configurations.

Syntax

```
[no] forward-proxy-failsafe-disable
```

Default This feature is enabled by default; use this command to disable SSLi failsafe.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-failsafe-disable
```

forward-proxy-inspect

Description Perform SSL Insight only if the traffic matches an entry in the specified class list. and is not bypassed by any other matching criteria. Only Aho-Corasick class-lists are supported by this command.

The **forward-proxy-inspect** criteria are applied first before any forward proxy bypass matching criteria. If `forward-proxy-inspect` is not configured, all SSL sessions are inspected for the other bypass matching criteria.

This command applies only to SSLi configurations.

Syntax

```
[no] forward-proxy-inspect class-list name
```

Parameter	Description
name	Class-list name (1-63 characters).

Mode SLB client SSL template configuration mode

Example The following example shows how the **forward-proxy-inspect** command works. In this example of an AC class-list, all URLs ending with `private.abc.com` will be bypassed, while all URLs ending with `public.abc.com` will go through SSLi processing.

```
ACOS# show config class-list
!Section configuration: 77 bytes
!
class-list my_class_list ac
  ends-with abc.com
  user-tag Security
!
ACOS# config
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# slb template client-ssl SSLi_vip_001_
client_ssl
ACOS(config-client ssl)# forward-proxy-inspect class-list my_
class_list
ACOS(config-client ssl)# forward-proxy-bypass contains
private.abc.com
```

Example The following example displays request processing under a combination of bypass and inspection configuration conditions.

Configuration

```
#sh run slb template client-ssl oym1
!Section configuration: 202 bytes
!
slb template client-ssl oym1
forward-proxy-ca-certificate ca1 key ca1
forward-proxy-enable
forward-proxy-bypass class-list b-class
forward-proxy-inspect class-list i-class
!
```

Class list contents

```
class-list b-class equals b.sample-a.ma
class-list i-class equals b.sample-a.ma
request is b.sample-a.ma, the request is bypassed.
```

Selection Results

forward-proxy-Inspect class-list b-class	forward-proxy-bypass class-list i-class	Actual request	Decision
b.sample-a.ma	b.sample-a.ma	b.sample-a.ma	Bypass
sample-a.ma	b. sample-a.ma	b.sample-a.ma	Bypass
sample-a.ma	b.sample-a.ma	a.sample-a.ma	Inspected
b.sample-a.ma	sample-a.ma	b.sample-a.ma	Inspected

forward-proxy-inspect certificate-issuer

Description Configures SSLi inspect based on the class-list from a certificate issuer.

Syntax `[no] forward-proxy-inspect certificate issuer class-list` *class_list_name*

Parameter	Description
class-list class_list_name	Inspects SSLi if the certificate issuer matches the class-list name.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi inspect based on class-list from a certificate issuer. To determine the Certificate Authority that issued your certificate, open the website in a browser and click on the certificate information.

Example Example Configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-inspect certificate-issuer class-list Nortan
```

forward-proxy-inspect certificate-san

Description Configures SSLi inspect based on the class-list from a certificate Subject Alternative Name (SAN).

Syntax

```
[no] forward-proxy-bypass certificate-san class-list class_list_name
```

Parameter	Description
class-list class_list_name	Inspects SSLi if the certificate SAN matches the class-list name.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi inspect based on class-list from a certificate SAN. This can secure a number of fully qualified domain names with a single certificate. You can specify additional host names

such as sites, IP addresses, common names, and so on, to be protected by a single SSL Certificate.

Example Example Configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-inspect certificate-san class-list xyzbank
```

forward-proxy-inspect certificate-subject

Description Configures SSLi inspect based on the class-list from a certificate subject.

Syntax `[no] forward-proxy-inspect certificate-subject class-list class_list_name`

Parameter	Description
class-list *class_list_name*	Inspects SSLi when the certificate subject matches the class-list name. You can enter only one class list name.

Default None

Mode SLB client SSL template configuration mode

Usage Use this command to enable SSLi inspect based on the class-list from a certificate subject.

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-inspect certificate-subject class-list Nortan
```

forward-proxy-log-disable

Description Disable SSL forward proxy (SSLi) logging.

This command applies only to SSLi configurations.

Syntax `[no] forward-proxy-log-disable`

Default SSLi logging is enabled by default; use this command to disable SSLi logging.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-log-disable
```

forward-proxy-no-shared-cipher-action

Description Specify the action taken if the handshake fails due to no shared cipher.

Syntax `[no] forward-proxy-no-shared-cipher-action {bypass | drop}`

Parameter	Description
bypass	Bypasses the connection. **NOTE:** This command is not supported in the SSLi and proxy-chain configurations.
drop	Drops the connection.

Default drop

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-no-shared-cipher-action
bypass
```

forward-proxy-no-sni-action

Description Specify the SSL forward proxy action in case of no SNI.

Syntax `[no] forward-proxy-no-sni-action {intercept | bypass | reset}`

Parameter	Description
bypass	Bypasses the connection.
intercept	Intercepts the connection.
reset	Resets the connection.

Default Intercept

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-no-sni-action bypass
```

forward-proxy-ocsp-disable

Description Disable OCSP Stapling for SSL forward proxy (SSLi).

This command applies only to SSLi configurations.

Syntax

```
[no] forward-proxy-ocsp-disable
```

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-ocsp-disable
```

forward-proxy-require-sni-cert-matched

Description Enable to match SNI in ClientHello message and subject CN/SANs in server certificate to prevent spoofing.

Syntax

```
[no] forward-proxy-require-sni-cert-matched {no-match-action-inspect | no-match-action-drop}
```

Parameter	Description
no-match-action-inspect	If client SNI does not match one of server certificate subject CN or DNS fields in SAN, then inspect the action.

Parameter	Description
no-match-action-drop	If client SNI does not match one of server certificate subject CN or DNS fields in SAN, then drop the action.

Default Disabled

Mode SLB client SSL template configuration mode

Usage Use this command to match SNI in ClientHello message and subject CN/SANs in server certificate to prevent spoofing.

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# fforward-proxy-require-sni-cert-matched no-match-action-drop
```

forward-proxy-selfsign-redir

Description With this option enabled, ACOS redirects traffic away from the self-signed site and to a warning page in which the client sees “The page you have tried to reach uses an untrusted certificate, please contact your administrator.”

This command applies only to SSLi configurations.

Syntax

```
[no] forward-proxy-selfsign-redir
```

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-selfsign-redir
```

forward-proxy-source-nat

Description To provision the SSL-Client template for source NAT.

Syntax

```
[no] forward-proxy-source-nat {pool pool-name [precedence] | auto [precedence]}
```

Parameters	Description
pool *pool-name*	When a fetched SSL session is connected and the source NAT *pool* option is configured, the ACOS Device replaces the client source IP address of forwarded SSLi traffic with an address from the specified NAT pool.
auto	When a fetched SSL session is connected and the source NAT *auto* option is configured, the ACOS Device replaces the client source IP address of forwarded SSLi traffic with the address of the real server that is forwarding traffic to the SSL server.
precedence	Enables source NAT configuration that is defined in the client SSL template to have a higher priority than the source NAT defined in the SLB policy template.

Default Disabled

Mode SLB client SSL template configuration mode

Usage This command applies only to SSLi configurations.

Example The following example configures dynamic IP addresses for source NAT in the SSL-Client template:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-source-nat auto
```

Example The following example configures static IP addresses for source NAT in the SSL-Client template with precedence set for source NAT:

```
ACOS(config)# slb template client-ssl c-ssl2
ACOS(config-client ssl)# forward-proxy-source-nat pool p3
precedence
```

forward-proxy-ssl-version

Description Specify the version of SSL to be used with SSL Insight.

Syntax `[no] forward-proxy-ssl-version {31 | 32 | 33 | 34}`

Parameter	Description
31	SSL/TLS v1.0.
32	SSL/TLS v1.1.
33	SSL/TLS v1.2. (default)
34	SSL/TLS v1.3.

Default 33

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-ssl-version 34
```

forward-proxy-trusted-ca

Description File in PEM format listing all the trusted CA certificates. When server verification is configured using this list, the action is to drop client connections if the certificate of the outside server is not on the trusted list.

This command applies only to the CA certs that are proxied for on the ACOS device for the interception of SSL sessions in SSLi (that is, forward-proxy) configurations.

NOTE: Additionally, you can update the 'a10_autoupdate_ca' CA bundle file for shared partition from the GLM server using the **automatic-update**command. For more information, refer to *Command Line Reference Guide*.

Syntax

```
[no] forward-proxy-trusted-ca file[partition shared]
```

Parameter	Description
file	Trusted CA file name (1-255 characters).
partition shared	Bind shared partition's certificate in private partition's client-SSL template.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-trusted-ca new_self.crt
ACOS(config-client ssl)# forward-proxy-trusted-ca
trustedCAs.pem
```

forward-proxy-verify-cert-fail-action

Description Configure the action of the client connection if CRL verification of any certificate fails. The options available are bypassing SSL Proxy, continuing with the connection, or dropping the connection.

This command applies only to the certs that are forged on the ACOS device for the interception of SSL sessions in SSLi configurations.

Syntax

```
[no] forward-proxy-verify-cert-fail-action
{block | bypass | continue | drop}
```

Default By default, the client connection is dropped if CRL verification of any certificate in the chain is not successful.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-verify-cert-fail-action
bypass
```

handshake-logging-enable

Description Enable SSL handshake logging.

Syntax

```
[no] handshake-logging-enable
```

Default Not enabled.

Mode SLB client-SSL template

Example Enable this feature:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# handshake-logging-enable
```

hsm-param

Description Specify HSM parameters.

Syntax

```
[no] hsm-param {thales-embed | thales-hwcrhk}
```

Parameter	Description
thales-embed	Thales embed key.
thales-hwcrhk	Thales hwcrhk key.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# hsm-param thales-embed
```

ja3-enable

Description Enable JA3 fingerprinting calculation for TLS client connections.

Syntax

```
[no] ja3-enable
```

Mode SLB client SSL template configuration mode

Example The following example enables this feature.

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# ja3-enable
```

Related Commands:

- ja3-insert-http-header
- ja3-reject-class-list
- ja3-reject-max-number-per-host

ja3-insert-http-header

Description Inserts JA3 MD5 string as a HTTP header and forward it to the back end HTTP server.

NOTE: Since the server is HTTP, the traffic must be HTTPS, and the SSLi or SSL offload must be configured, otherwise the header cannot be inserted.

Syntax

```
[no] ja3-insert-http-header {HTTP_header_name}
```

Parameter	Description
HTTP_header_name	Specify the HTTP header name.

Default Not set

Mode SLB Client-SSL template Configuration Mode

Example The following example enables this feature.

```
ACOS(config)#slb template client-ssl clientssl
ACOS(config-client ssl)# ja3-enable
ACOS(config-client ssl)# ja3-insert-http-header X-JA3
```

Related Commands:

- ja3-enable
- ja3-reject-class-list
- ja3-reject-max-number-per-host

ja3-reject-class-list

Description Configure this option to reject SSL/TLS connections by class-list containing JA3 fingerprints of the known malicious clients.

Syntax

```
[no] ja3-reject-class-list {class-list_name}
```

Parameter	Description
class-list_name	Specify the name of the class-list. The class-list must be of string-case-insensitive type only.

Default Not set

Mode SLB client SSL template Configuration Mode

Usage If JA3 of the current connection matches any member in the class-list, then SSL rejects this connection.

Example The following example configures this feature:

```
ACOS(config)#class-list JA3-BLOCK string-case-insensitive
ACOS(config-class list)# str F436B9416F37D134CADD04886327D3E8
ACOS(config-class list)# exit
ACOS(config)#slb template client-ssl clientssl
ACOS(config-client ssl)# ja3-enable
ACOS(config-client ssl)# ja3-reject-class-list JA3_BLOCK
```

Related Commands:

- ja3-enable
- ja3-insert-http-header
- ja3-reject-max-number-per-host

ja3-reject-max-number-per-host

Description Configure a number as the maximum of JA3 amount in each client address.

Syntax `[no] ja3-reject-max-number-per-host max_num ttl ttl_value`

Parameter	Description
max_num	Specify the maximum number of JA3 amount per host. The request will drop if the number of JA3 of this client address exceeds.
ttl *ttl_value*	Specify the TTL value to retain each JA3 record. By default, the value is set to 600. The value can be between 1-86400.

Default Not set

Mode SLB Client-SSL template Configuration Mode

Usage If the JA3 amount of client address exceeds this value, then SSL rejects this connection.

Example The following example enables this feature.

```
ACOS(config)#slb template client-ssl clientssl
ACOS(config-client ssl)# ja3-enable
ACOS(config-client ssl)# ja3-reject-max-number-per-host 4 ttl
340
```

Related Commands:

- ja3-enable
- ja3-insert-http-header
- ja3-reject-class-list

ja4-enable

Description Enables JA4 fingerprinting method for TLS client connections.

Syntax

```
[no] ja4-enable
```

Mode SLB client SSL template configuration mode

Usage JA4+ is a successor to the JA3 TLS fingerprinting method, which uses both human and machine-readable fingerprinting techniques. JA4+ examines the TLS Client Hello packet and builds a fingerprint for the client based on various attributes within the packet.

Example The following example enables JA4 feature.

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# ja4-enable
```

Related Commands:

- ja3-insert-http-header
- ja3-reject-class-list
- ja3-reject-max-number-per-host
- ja4-insert-http-header
- ja4-reject-class-list
- ja4-reject-max-number-per-host

ja4-insert-http-header

Description Inserts JA4 hash as a HTTP header and forwards it to the back end HTTP server.

NOTE: Since the server is HTTP, the traffic must be HTTPS, and the SSLi or SSL offload must be configured, otherwise the header cannot be inserted.

Syntax

```
[no] ja4-insert-http-header {HTTP_header_name}
```

Parameter	Description
HTTP_header_name	Specify the HTTP Header Name length. The length can be between 1 to 128 characters.

Default Not set

Mode SLB Client-SSL template Configuration Mode

Example The following example enables this feature.

```
ACOS(config)#slb template client-ssl clientssl
ACOS(config-client ssl)# ja4-enable
ACOS(config-client ssl)# ja4-insert-http-header X-JA3
```

Related Commands:

- ja3-enable
- ja3-reject-class-list
- ja3-reject-max-number-per-host
- ja4-enable
- ja4-reject-class-list
- ja4-reject-max-number-per-host

ja4-reject-class-list

Description Configure this option to reject SSL/TLS connections by class-list containing JA4 fingerprints of the known malicious clients.

Syntax

```
[no] ja4-reject-class-list {class-list_name}
```

Parameter	Description
class-list_name	Specify the name of the class-list. The class-list must be of string-case-insensitive type only.

Default Not set

Mode SLB client SSL template Configuration Mode

Usage If JA4 of the current connection matches any member in the class-list, SSL rejects this connection.

Example The following example configures this feature:

```
ACOS(config)#class-list JA4-BLOCK string-case-insensitive
ACOS(config-class list)# str F436B9416F37D134CADD04886327D3E8
ACOS(config-class list)# exit
ACOS(config)#slb template client-ssl clientssl
ACOS(config-client ssl)# ja4-enable
ACOS(config-client ssl)# ja4-reject-class-list JA4_BLOCK
```

Related Commands:

- ja3-enable
- ja3-insert-http-header
- ja3-reject-max-number-per-host
- ja4-enable
- ja3-insert-http-header
- ja4-reject-max-number-per-host

ja4-reject-max-number-per-host

Description Configure a number as the maximum of JA4 amount in each client address.

Syntax

```
[no] ja4-reject-max-number-per-host max_num ttl ttl_value
```

Parameter	Description
max_num	Specify the maximum number of JA4 amount per

Parameter	Description
	host. The request will drop if the number of JA4 of this client address exceeds.
ttl *ttl_value*	Specify the TTL value to retain each JA4 record. By default, the value is set to 600. The value can be between 1-86400.

Default Not set

Mode SLB Client-SSL template Configuration Mode

Usage If the JA4 amount of client address exceeds this value, SSL rejects this connection.

Example The following example enables this feature.

```
ACOS(config)#slb template client-ssl clientssl
ACOS(config-client ssl)# ja4-enable
ACOS(config-client ssl)# ja4-reject-max-number-per-host 4 ttl
340
```

Related Commands:

- ja3-enable
- ja3-insert-http-header
- ja3-reject-class-list
- ja4-enable
- ja3-insert-http-header
- ja3-reject-class-list

local-logging

Description Enables local loggin.

Syntax `[no] local logging`

Default Disabled

Mode SLB Client SSL configuration mode

Example The following command sets the low-latency:

```
ACOS(config)# slb template client-ssl clientSSL
ACOS(config-client ssl)# local-logging
```

non-ssl-bypass

Description Specifies that non-SSL session traffic is redirected to the specified service group.

Syntax

```
[no] non-ssl-bypass service-group name
```

Parameter	Description
name	Service group name (1-127 characters).

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# non-ssl-bypass service-group Non_SSL_
sg1
```

ocsp-stapling

Description Configure OCSP Stapling support.

Syntax

```
[no] ocsp-staplingca-certcert-nameocsp
{auth-server-name | service-groupgroup-name}
[period [daysnum | hoursnum | minutesnum]
[timeoutminutes]
```

Parameter	Description
cert-name	CA certificate name.
auth-server-name	OCSP authentication server name (1-63 characters).
group-name	OCSP authentication service-group name (1-127 characters).

Parameter	Description
period	Specifies how often ACOS contacts the server or service group for updates. Default is 1 hour.
timeout	Specifies the timeout for server retries, 1-65535. Default is 30 minutes.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# ocsp-stapling ca-cert MyCACert ocsp
AuthServerName period hours 2
```

renegotiation-disable

Description Disable automatic TLS/SSL renegotiation.

ACOS allows for renegotiation of SSL connections over previously secured channels to help speed up the re-establishment of previous SSL connections with known clients. Disabling TLS/SSL renegotiations can help prevent vulnerabilities that may lead to SSL/TLS renegotiation Man-In-TheMiddle Attacks.

Syntax

```
[no] renegotiation-disable
```

Default TLS/SSL renegotiations are enabled by default.

Mode SLB client SSL template configuration mode

require-sni-cert-matched

Description Enable to match SNI in the ClientHello message and domain names (in CN and SAN DNS fields) in configured certificates to prevent unnecessary information leak to the client.

Syntax

```
[no] require-sni-cert-matched
```

Default Disabled

Mode SLB client SSL template configuration mode

Usage Use this command to match SNI in the ClientHello message and domain names (in CN and SAN DNS field) in the configured certificates to prevent unnecessary information leak to the client.

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# require-sni-cert-matched
```

server-name

Description Configure Server Name Indication (SNI) in the client Hello extension.

A second certificate can be assigned to the server with the alternate option. Two certificates assigned to a template must be of different types (RSA, ECDSA). A major (first) certificate must be assigned before an alternate (second) certificate is accepted by the template.

When the command includes a chain cert, the SNI SSL ctx is configured with the cert and chain cert. When a default chain cert is defined for the template, the default chain cert is used in place of the configured chain.

Syntax

```
[no] server-name server-name cert cert-name [chain chain-name]
key key-name [pass-phrase string [alternate | partition
shared]
```

Parameter	Description
server-name	Server name string (1-63 characters).
cert-name	Server certificate associated to SNI (1-255 characters).
chain-name	Chain certificate associated to SNI
key-name	Server private key associated to SNI (1-255 characters).

Parameter	Description
string	Help password phrase (1-128 characters).
alternate	Specifies a second (or backup) certificate and key.
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# server-name SNIServer cert SNICert
key SNIKey pass-phrase SNIHelp
```

server-name-auto-map

Description Enables dynamic SNI extension support. When this option is enabled, SNI-based ctx creation (SSL context) is enabled. The SSL context is created based on the SNI in the client hello if a cert and key was previously imported to the device.

The *no server-name-auto-map* command disables dynamic SNI extension support.

Syntax

```
[no] server-name-auto-map [enable-log]
```

Parameter	Description
enable-log	Logging of SNI auto mapping failures is enabled. When this parameter is not included, SNI auto mapping failure logging is disabled

Default Disabled

Mode SLB client SSL template configuration mode

Usage When dynamic SNI extension support is enabled, a matching cert and key is required for inbound client hello SNI contents. For example, for the sni www.a10networks-black.com, then the following files are required:

- Imported cert: www.a10networks-black.com.crt

- Imported key: www.a10networks-black.com.key

Example

This example imports a cert and key file for the www.a10networks-green.com file, then enables dynamic SNI extension support.

```
ACOS(config)# import key www.a10networks-green.com.key
scp://10.1.1.1/green.key
ACOS(config)# import cert www.a10networks-green.com.cert
scp://10.1.1.1/green.cert
ACOS(config)# slb template client-ssl CLIENT-1
ACOS(config-client ssl)# server-name-auto-map
ACOS(config-client ssl)# exit
ACOS(config)# show run | sec slb template client-ssl
slb template client-ssl CLIENT-1
  server-name-auto-map
ACOS(config)#
```

server-name-regex

Description

Configure Server Name Indication (SNI) in the ClientHello extension with regular expressions.

Syntax

```
[no] server-name-regex server-name cert cert-name [chain
chain-name] key  key-name [pass-phrase string] [alternate |
partition shared]
```

Parameter	Description
server-name-regex	Server name string with regular expression (1-63 characters). **NOTE:** The string supports the '\\' characters. For example, if you enter the test \.com, ACOS converts it to "\\.com".
cert-name	Server certificate associated to SNI (1-255 characters).
chain-name	Chain certificate associated to SNI.
key-name	Server private key associated to SNI (1-255 characters).

Parameter	Description
string	Help password phrase (1-128 characters).
alternate	Specifies a second (or backup) certificate and key.
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.

Mode SLB client SSL template configuration mode

Usage The wildcard support includes the following regular expression symbols:

```
^ $ . | * + [ {
```

Usage of the following symbols is not supported:

```
? ( ) \
```

When a new connection request is made from client, the SNI from TLS extension in ClientHello is captured and first checked against "server-name" config with existing hash method. If no match found, it is compared with the compiled regex string configured by server-name-regex. When multiple server-name-regex entries match, the cert/key associated with the best match is used.

A second certificate can be assigned to the server with the alternate option. Two certificates assigned to a template must be of different types (RSA, ECDSA). A major (first) certificate must be assigned before an alternate (second) certificate is accepted by the template.

When the command includes a chain cert, the SNI SSL ctx is configured with the cert and chain cert. When a default chain cert is defined for the template, the default chain cert is used in place of the configured chain.

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# server-name SNIServer cert SNICert
key SNIKey pass-phrase SNIHelp
```

Example These commands configure a client-SSL template that uses a wildcard entry as the fully qualified domain name, thereby binding many server names in client hello extensions with one certificate and key configuration. In this example, the regex characters allow a match on www.exaple.com or www.exmple.com.

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# server-name-regex www.ex[am]ple.com
cert cert1 key cert1
```

Related Commands:

- show run slb template

server-name-bypass

Description Enable SNI bypass.

This command is available only if one of the below commands are configured:

- server-name
- server-name-regex
- server-name-auto-map

Syntax

```
[no] server-name-bypass {missing-cert | expired-cert |
explicit-class-list class-list | enable-log}
```

Parameter	Description
missing-cert	Bypass the SSL traffic when the SNI does not match with any of the configured server names.
expired-cert	Bypass SSL traffic when SNI matches one of the server-names, but the certificate is expired.
explicit-class-list *class-list*	Bypass SSL traffic when the SNI is specified in the class-list. This command only accepts the AC type class-list.
enable-log	Generate the log when the SNI bypasses.

Default Disabled

Mode SLB client SSL template configuration mode

Usage When the server-name is configured under client-SSL template, and you want to bypass SSL traffic in the following scenarios:

- Missing cert/key, i.e., client SNI does not match
- Client SNI matches one of the configured server-name, but the certificate is expired
- Client SNI matches the configured SNI bypass class-list

Example This example enables SNI bypass.

```
ACOS(config)# slb template client-ssl clissl
ACOS(config-server ssl)# certificate Cert123.pem key key123
pass-phrase Pass123
ACOS(config-client ssl)# server-name-auto-map enable-log
ACOS(config-client ssl)# server-name-bypass missing-cert
ACOS(config-client ssl)# server-name-bypass expired-cert
ACOS(config-client ssl)# server-name-bypass explicit-class-
list sni_bypass
ACOS(config-client ssl)# server-name-bypass enable-log
```

session-cache-size

Description Maximum number of cached sessions for SSL session ID reuse.

Syntax

```
[no] session-cache-size entries
```

Parameter	Description
entries	Number of entries. The range of values allowed is from 0 to a maximum dependent on the platform on which ACOS is running. The value 0 disables session ID reuse.

Default The default is 0; session ID reuse is disabled.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# session-cache-size 1000
```

session-cache-timeout

Description Sets the maximum number of seconds a cache entry can remain unused before being removed from the cache. Cache entries age according to the ticket age time. The age time is not reset when a cache entry is used.

Syntax

```
[no] session-cache-timeout seconds
```

Parameter	Description
seconds	Number of seconds (0 - 604800 seconds).

Mode SLB client SSL template configuration mode

Default The default is 0; session cache timeout is disabled.

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# session-cache-timeout 5400
```

session-key-logging-enable

Description Enables SSL session key logging.

Syntax

```
[no] session-key-logging-enable
```

Default Feature is not enabled.

Mode SLB client SSL template configuration mode

Example Enable SSL session key logging feature:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# session-key-logging-enable
```

session-ticket-disable

Description Disables client side SSL session ticketing.

Syntax `[no] session-ticket-disable`

Default By default, this is not set.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# session-ticket-disable
```

session-ticket-lifetime

Description Sets the lifetime for stateless SSL session ticketing. After a client's SSL ticket expires, they must complete an SSL handshake in order to set up the next secure session with ACOS.

NOTE: This option is supported on sofware, software TLS1.3, QAT, and new N5 SSL modules.

Syntax `[no] session-ticket-lifetime seconds`

Parameter	Description
seconds	Number of seconds. Setting the lifetime to 0 disables the feature.

Default Disabled.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# session-ticket-lifetime 7200
```

ssl-false-start-disable

Description SSL False Start support for Google Chrome browser.

NOTE: The following ciphers are not supported for SSL False Start in the current release:

SSL3_RSA_DES_64_CBC_SHA
SSL3_RSA_RC4_40_MD5
TLS1_RSA_EXPORT1024_RC4_56_MD5

If no other ciphers but these are enabled in the client-SSL template, SSL False Start handshakes will fail.

Syntax `[no] ssl-false-start-disable`

Default SSL false start is enabled by default.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template client-ssl clientssl
ACOS(config-client ssl)# ssl-false-start-disable
```

ssli-inbound-enable

Description Enables the SNI information transmission in the inbound SSLi.

NOTE: This option cannot work if the source NAT feature is enabled on the client SSL template in inbound SSLi.

Prerequisite

- Enable the ssli-sni-hash-enable command.

Syntax `[no] ssli-inbound-enable`

Default Disabled

Mode SLB Client SSL Template

Usage Use this feature only when you want to relay the SNI information from the client-side inbound SSLi to the server-side outbound SSLi. The inbound SSLi preserves the client-side SNI information, relays it to the server-side, and completes the SSL/TLS negotiation.

This option applies to all the SSLi topologies. It is also works for non-HTTP and HTTP applications that lack 'HOST' header information.

Example The following example enables the SNI information transmission in inbound SSLi:

```
ACOS(config)# slb template client-ssl inbound_ssli
ACOS(config-client ssl)# ssli-inbound-enable
```

Related Commands:

- ssli-sni-hash-enable clientside-ip | clientside-ipv6
- ssli-sni-hash-enable serverside-ip | serverside-ipv6

ssli-logging

Description Enables or disables SSLi logging for all SSLi events.

For more information on SSLi logging, see *SSL Insight Configuration Guide*.

Syntax

```
[no] ssli-logging { disable | all }
```

Parameter	Description
disable	Disables SSLi logging for all events, including success and failure.
all	Enables SSLi logging for all events, including success and failure.

Default By default, SSLi logging is enabled to capture error level logs.

NOTE:

Although the default SSLi logging captures error level logs only, there is one exception. In case the forward-proxy-bypass is configured, the 'info' level logs are also captured for 'SSL Inspection Bypassed.'

This additional logging occurs because 'inspection' is considered as standard setting, while 'bypass' (no inspection) is considered as exception handling setting. Therefore, you should treat such log as an exception information rather than an error log.

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# ssli-logging all
```

sslv2-bypass

Description Redirects clients who request SSLv2 sessions to the specified service group.

Syntax `[no] sslv2-bypass service-group service-group-name`

Parameter	Description
service-group-name	Name of the service group (1-127 characters).

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# sslv2-bypass service-group SSLv2_SG
```

template

Description Name of a cipher or HSM template to bind to client-SSL and server-SSL templates. In this case, the settings in the cipher template override any cipher settings in the client-SSL template.

Syntax `[no] template {cipher template-name | hsm template-name}`

Parameter	Description
cipher	SLB cipher template name (1-63 characters).
hsm	HSM template name (1-63 characters).

Mode SLB client SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template client-ssl clientssl
```

```
ACOS(config-client ssl)# template cipher SLB_Cipher_Template
```

version

Description Specifies the security version and minimum allowable security version that can be used when communicating with SSL clients and servers.

In SSLi configurations, the security version from this template must match the security version configured under the client-SSL template through the forward-proxy-ssl-version command.

Syntax

```
[no] version {version-num} [downgrade-version-num]
```

Parameter	Description
version-num	Select one of the following: • 30 - Secure Sockets Layer (SSL) v3.0 • 31 - Transport Layer Security (TLS) v1.0 • 32 - Transport Layer Security (TLS) v1.1 • 33 - Transport Layer Security (TLS) v1.2 • 34 - Transport Layer Security (TLS) v1.3
downgrade-version-num	Specifies the minimum SSL/TLS version to which a session can be downgraded. To disable downgrading, specify the same version number for both the *version-num* and *downgrade-version-num*

Default 34

Mode SLB client SSL template configuration mode

Example The following example configures TLS version 1.1 for use in SSL communication with the clients. Depending on the response received from each client, TLS version 1.0 may also be used.

```
ACOS(config)# slb template client-ssl SSL
ACOS(config-client ssl)# version 32 31
```

Example The following example disables downgrade; only TLS version 1.2 can be used to communicate with clients. If the client is using a lower (less secure) version of TLS, the session will not be created.

```
ACOS(config)# slb template client-ssl SSL
ACOS(config-client ssl)# version 33 33
```

slb template client-ssh

Description Names an SSH client template and enters the configuration mode where you can enable SSH client services, such as validation of SSH clients.

Syntax

```
[no] slb template client-ssh template-name
```

Replace *template-name* with the name of the template, up to 31 characters long.

This command enters the SLB Client-SSH Template configuration mode.

Default If none of the SSH Client template sub-commands in the preceding table are configured, the default action of the SSH Client template is the combined default actions of the individual SSH Client sub-commands.

Mode Global configuration mode

Usage The normal form of this command creates a client-SSH configuration template. The **no** form of this command removes the template.

Example The following commands configure a client-SSH template named **SSHInsight_ClientSide** that uses RSA_key_1234:

```
ACOS-Inside(config)#slb template client-ssh SSHInsight_
ClientSide
ACOS-Inside(config client-ssh)#forward-proxy-hostkey RSA_key_
1234
ACOS-Inside(config-client-ssh)#forward-proxy-enable
```

You can bind only one client-SSH template to a virtual port. However, you can bind the same client-SSH template to multiple virtual ports.

```
ACOS-Inside(config)#slb virtual-server Inside_VIP 0.0.0.0 acl
100
ACOS-Inside(config-slb vserver)#port 22 ssh
```

```
ACOS-Inside(config-slb vserver-vport)#service-group FW1_
Inspect_SG
ACOS-Inside(config-slb vserver-vport)#no-dest-nat port-
translation
ACOS-Inside(config-slb vserver-vport)#template client-ssh
SSHInsight_ClientSide
```

forward-proxy-enable

Description Enables SSH Insight (SSHi) support on ACOS SLB virtual server.

Syntax

```
[no] forward-proxy-enable
```

Mode SLB client SSH template configuration mode

Example Example configuration:

```
ACOS-Inside(config)#slb template client-ssh SSHInsight_
ClientSide
ACOS-Inside(config client-ssh)#forward-proxy-hostkey RSA_key_
1234
ACOS-Inside(config-client-ssh)#forward-proxy-enable
```

slb template server-ssl

Description Configure the ACOS device to validate real servers based on their certificates.

Syntax

```
[no] slb template server-ssl template-name
```

Parameter	Description
template-name	Template name (1-127 characters)

This command enters the SLB Server-SSL Template Configuration Mode for the specified server-ssl template.

Default The configuration does not have a default server-side SSL template.

Mode Global Configuration mode

Usage The normal form of this command creates a server-SSL configuration template.

The `no` form of this command removes the template.

You can bind only one server-SSL template to a virtual port. However, you can bind the same server-SSL template to multiple ports.

Usage Server-SSL Template Binding

ACOS supports use of a server-SSL template with only one instance of a real port. For example, if the same real server:port member is used in two service groups, it is valid to bind each of those service groups to a different virtual port. However, if there are server-SSL templates configured for both virtual ports, the server-side SSL behavior is not predictable and is not supported. It is recommended to duplicate the real server port configuration with different real servers in each group.

In the following example, an ACOS system is configurred with two virtual-servers, `SSL_Internet_vip_001` and `SSL_Internet_vip_003`. And, each of these virtual servers are configured with an HTTP virtual port, `port 8080 http`.

A different SSL-template and a different service group is applied to each virtual port.

- The SSL-template, `SSL_Internet_vip_001_server_ssl`, and the service group, `sg2`, are applied to `port 8080 http` on `SSL_Internet_vip_001`.

```
slb virtual-server SSL_Internet_vip_001 0.0.0.0 acl 1
  user-tag Security
  port 8080 http
    service-group sg2
    use-rcv-hop-for-resp
    template server-ssl SSL_Internet_vip_001_server_ssl
    no-dest-nat port-translation
```

- The SSL-template, `SSL_Internet_vip_003_server_ssl`, and the service group, `sg1`, are applied to `port 8080 http` on `SSL_Internet_vip_003`.

```
slb virtual-server SSL_Internet_vip_003 0.0.0.0 acl 3
```

```
  user-tag Security
  port 8080 http
    service-group sg1
    use-rcv-hop-for-resp
    template server-ssl SSL_Internet_vip_003_server_ssl
    no-dest-nat port-translation
```

- The preceding configuration is supported when each service group specifies a different real server. Service group `sg1` specifies real server, `rs1`, and service group, `sg2`, specifies real server, `rs2`:

```
slb server rs1 192.168.1.10
  port 80 tcp

slb server rs2 192.168.2.10
  port 80 tcp

slb service-group sg1 tcp
  member rs1 80
    template tcp1

slb service-group sg2 tcp
  priority-affinity
  member rs2 80
```

- However, the configuration is not supported when both service groups specify the same real server, `rs1`, as shown in the following:

```
slb server rs1 192.168.1.10
  port 80 tcp

slb service-group sg2 tcp
  member rs1 80
    template tcp1

slb service-group sg1 tcp
  priority-affinity
  member rs1 80
```

ca-cert

Description Specifies the name of a CA certificate. A server-SSL template can have multiple CA-signed certificates.

The ACOS device is configured at the factory with the CA certificate bundle file "default_ca_bundle," including common trusted certificate authorities. Use the **show pki ca-cert** command to view the list of ca-certificates.

You can add the CA certificates to the server-SSL template in either of the following ways:

- As separate files (one for each certificate)
- As a single file containing multiple certificates

Syntax

```
[no] ca-cert cert-name [partition shared]
[ocsp {ocsp-server-name | service-group ocsp-service-group-name}]
```

Parameter	Description
ca-cert-name	Name of the CA certificate (1-255 characters)
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.
ocsp-server-name	Name of the OCSP server (1-255 characters)
ocsp-service-group-name	Name of the OCSP service-group (1-255 characters)

Mode SLB server-SSL template

Usage If validation of the ca-cert fails, the connection to the server is terminated.

Example Specify "example.pem" as the name of the certificate:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# ca-cert example.pem
```

certificate

Description Specifies the name of the certificate and key name pair with optional pass-phrase setting, to use for terminating or initiating an SSL connection. The certificate and key must be installed, and available on the ACOS device.

NOTE: The certificate command is used to replace the old cert/cert-alternate/key/key-alternate/chain-cert command. The new certificate configuration cannot co-exist with these commands.

Syntax

```
[no] certificate <cert-name> key <key-name> [pass-phrase
<pass-phrase-str>] [chain-cert <chain-cert-name>] [partition
shared]
```

Parameter	Description
cert-name	CA certificate name (1-245 characters).
chain-cert-name	Specifies a certificate-key chain. Chain certificate name (1-245 characters). **NOTE:** If **chain-cert** parameter is required, then make sure to configure it in the same line of certificate and key.
pass-phrase	Specifies the password phrase (1-128 characters).
partition shared	Bind shared partition's alternate certificate in private partition's client-SSL template.

Mode SLB server-SSL template

Example Specify "example.pem" as the name of the certificate:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# certificate Cert123.pem key key123
pass-phrase Pass123
```

cipher

Description Specifies the cipher suite to support for certificates from servers.

You can remove (or re-add) one cipher in the template with a single command. Enter separate commands for each cipher to remove or re-add.

Syntax

```
[no] cipher name
```

Parameter	Description
name	Name of the cipher. The supported cipher are listed a axseries. or enter **cipher ?** from the command line.

Mode SLB server SSL template

Example Specify " SSL3_RSA_RC4_128_SHA " as the cipher:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# cipher SSL3_RSA_RC4_128_SHA
```

close-notify

Description Enables close notification (close_notify) alerts for SSL sessions.

NOTE: This command can not be used along with the TCP-proxy template **force-delete-timeout** option. Doing so may cause unexpected behavior.

Syntax

```
[no] close-notify
```

Default Disabled

Mode SLB server-SSL template

Usage When this command is enabled, the ACOS device sends a close_notify message when an SSL transaction ends, before sending a FIN. This behavior is required by certain types of applications, including PHP cgi.

NOTE: The **close-notify** option may not work if **connection reuse** is also configured on the same virtual port. In this case, when the server sends a FIN to the ACOS device, the ACOS device will not send a FIN followed by a close notification. Instead, the ACOS device will send a RST.

Example Enable this feature:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# close-notify
```

crl

Description Specifies the names of the Certificate Revocation Lists (CRLs) to use for verifying whether server certificates have been revoked. The CRLs must be installed on the ACOS device first. (Use the **import** command for more details). The CA certificate relevant to the CRL must also be specified.

Syntax

```
[no] crl crl_name [partition shared]
```

Parameter	Description
crl_name	CRL name (1-255 characters).
partition shared	Bind shared partition's CRL in the private partition's server-SSL template.

Mode SLB server SSL template configuration mode

Example Example Configuration:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-server ssl)# crl 10_ca.crt_crl.pem partition
shared
ACOS(config-client ssl)# ca-cert 10_ca_crt
```

dh-param

Description Specify Diffie-Hellman parameters.

Syntax

```
[no] dh-param {1024 | 1024-dsa | 2048}
```

Default Not enabled

Mode SLB server SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-client ssl)# dh-param 1024
```

early-data

Description Enable the early data (0-RTT) for SSL version TLSv1.3.

Additionally, you must configure either **session-cache-size** or **session-ticket-enable** to do PSK resumption.

NOTE:
- Supported on new N5 module, QAT module, and Software TLS 1 .3.
- Maximum value is set to 16384 once enabled and is non-editable.

Syntax **[no]early-data**

Default Not Enabled.

Mode SLB server SSL template configuration mode

Usage This allows the server to respond immediately by including the requested data in the Server Hello or Finished message.

Example The following command configures **early data** for server-SSL template, svr-0rtt-test:

```
ACOS(config)# slb template server-ssl svr-0rtt-test
ACOS(config-server ssl)# ec-name secp384r1
ACOS(config-server ssl)# close-notify
ACOS(config-client ssl)# session-ticket-enable
ACOS(config-client ssl)# version 34 33
ACOS(config-client ssl)# early-data
```

ec-name

Description Specify elliptic curve name.

Syntax [no] **ec-name** {**secp256r1** | **secp384r1**}

Default **secp256r1**

Mode SLB server-SSL template

Example Example Configuration:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-client ssl)# ec-name secp384r1
```

enable-ssli-ftp-alg

Description Enables FTP passive mode over TLS support for the specified port number. The port number value can between 1-65535.

NOTE: This configuration is applicable for implicit FTPS.

Syntax `[no] enable-ssli-ftp-alg port-num {<1-65535>}`

Default Disabled.

Mode SLB server SSL template configuration mode

Example Example configuration:

```
ACOS(config)#  slb template server-ssl serverssl
ACOS(config-client ssl)# enable-ssli-ftp-alg 990
```

enable-tls-alert-logging fatal

Description Enables logging of TLS alerts that include the flow information such as source IP address.

Syntax `[no] enable-tls-alert-logging fatal`

Default Not enabled.

Mode SLB server-SSL template

Example Enable this feature:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# enable-tls-alert-logging fatal
```

forward-proxy-enable

Description Enables SSL Insight support.

Syntax `[no] forward-proxy-enable`

Default Not enabled.

Mode SLB client SSL and server SSL template configuration mode

Example Enable this feature:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# forward-proxy-enable
```

handshake-logging-enable

Description Enable SSL handshake logging.

Syntax `[no] handshake-logging-enable`

Default **Not enabled.**

Mode SLB server-SSL template

Example Enable this feature:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-client ssl)# handshake-logging-enable
```

ocsp-stapling

Description Enable OCSP stapling support.

Syntax `[no] ocsp-stapling`

Default Not enabled.

Mode SLB server SSL template configuration mode

Example Enable this feature:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-client ssl)# ocsp-stapling
```

renegotiation-disable

Description Disables TLS/SSL renegotiation.

Syntax `[no] renegotiation-disable`

Default TLS/SSL secure renegotiation is enabled.

Mode SLB server-SSL template

Usage TLS/SSL secure renegotiation is disabled if the `renegotiation-disable` command is entered in both the SLB server-SSL and SLB client-SSL templates. The `no renegotiation-disable` command entered in both templates re-enables secure renegotiation.

Usage TLS/SSL secure renegotiation is enabled if the `no renegotiation-disable` command is entered in both the SLB server-SSL template and the SLB client-SSL template.

Example Disable TLS/SSL renegotiation:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# renegotiation-disable
```

server-certificate-error

Description Specifies the ACOS response if there is a server certificate error.

Syntax

```
[no] server-certificate-error {email | ignore | logging | trap}
```

Parameter	Description
email	Send an Email.
ignore	Ignore the error and allow traffic.
logging	Generate a log message.
trap	Generate an SNMP trap.

Default Not set; the connection is refused without any notification.

Mode SLB server-SSL template

Example Send an SNMP trap when there is a server certificate error:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# server-certificate-error trap
```

server-name

Description Configure a user-defined server name to the server side of an SSL proxy configuration.

Syntax

```
[no] server-name <server_name>
```

Default User defined name is not passed through to the server-side.

Mode SLB server-SSL template

Example The following example shows the server side template in an ACOS SSL proxy configuration where the user-defined server name is passed through to the SSL server:

```
ACOS(config)# slb template server-ssl test
ACOS(config-server ssl)# server-name www.test.com
ACOS(config-server ssl)# no server-name www.test.com
```

session-cache-size

Description Sets the maximum number of session-ID entries.

Syntax

```
[no] session-cache-size num
```

Parameter	Description
num	Number of session-ID entries. Specify 0 to disable caching.

Default Not enabled.

Mode SLB server-SSL template

Example Specify 5000000 entries:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# session-cache-size 5000000
```

session-cache-timeout

Description Sets the maximum number of seconds a cache entry can remain unused before being removed from the cache.

Cache entries age according to the ticket age time. The age time is not reset when a cache entry is used. After a client's SSL ticket expires, they must complete an SSL handshake in order to set up the next secure session with ACOS.

Syntax

```
[no] session-cache-timeout num
```

Parameter	Description
num	Number of seconds.

Default Not enabled.

Mode SLB server-SSL template

Example Specify 5000 seconds as the timeout value:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# session-cache-timeout 5000
```

session-key-logging-enable

Description Enables SSL session key logging.

Syntax

```
[no] session-key-logging-enable
```

Default Feature is not enabled.

Mode SLB server-SSL template

Example Enable SSL session key logging feature:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# session-key-logging-enable
```

session-ticket-enable

Description Enables stateless SSL session ticketing features.

Syntax

```
[no] session-ticket-enable
```

Default Feature is not enabled.

Mode SLB server-SSL template

Example Enable stateless SSL session ticketing features:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# session-ticket-enable
```

ssli-logging

Description Enables or disables SSLi logging for all SSLi events.

Syntax

```
[no] ssli-logging { disable | all }
```

Parameter	Description
disable	Disables SSLi logging for all events, including success and failure.
all	Enables SSLi logging for all events, including success and failure.

Default By default, SSLi logging is enabled to capture error level logs.

NOTE:

Although the default SSLi logging captures error level logs only, there is one exception. In case the forward-proxy-bypass is configured, the 'info' level logs are also captured for 'SSL Inspection Bypassed.'

This additional logging occurs because 'inspection' is considered as standard setting, while 'bypass' (no inspection) is considered as exception handling setting. Therefore, you should treat such log as an exception information rather than an error log.

Mode SLB server SSL template configuration mode

Example Example configuration:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-server ssl)# ssli-logging all
```

template cipher

Description Name of a cipher template to bind to the server-SSL template. In this case, the settings in the cipher template override any cipher settings in

the server-SSL template.

Syntax

```
[no] template cipher name
```

Parameter	Description
name	Name of the cipher template (1-63 characters).

Default Not set; the ciphers enabled in the server-SSL template are used.

Mode SLB server-SSL template

Example Bind the cipher template “cipher-tmp1” to this server-SSL template:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# template cipher cipher-tmp1
```

use-client-sni

Description Pass the client domain name to the server side of an SSL proxy configuration.

Syntax

```
[no] use-client-sni
```

Default Client domain name is not passed through to the server-side.

Mode SLB server-SSL template

Example The following example shows the server side template in an ACOS SSL proxy configuration where the client domain name is passed through to the SSL server:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# use-client-sni
```

version

Description Specify the security version.

Syntax

```
[no] version num1 num2
```

Parameter	Description
num1	This is the default security version.
num2	This is the lowest security version. You can downgrade the security version.

The available versions are 30, 31, 32, 33 and 34.

Parameter	Description
30	Secure Sockets Layer (SSL) v3.0.
31	Transport Layer Security (TLS) v1.0.
32	Transport Layer Security (TLS) v1.1.
33	Transport Layer Security (TLS) v1.2
34	Transport Layer Security (TLS) v1.3

Default 34

Mode SLB server-SSL template

Example Use TLS v1.1 security:

```
ACOS(config)# slb template server-ssl sstmp1
ACOS(config-server ssl)# version 32 32
```

slb template server-ssh

Description Configure the ACOS device to validate real SSH servers based on their certificates.

Syntax

```
[no] slb template server-ssh template-name
```

Parameter	Description
template-name	Template name (1-31 characters)

This command enters the SLB Server-SSH Template Configuration Mode for the specified server-ssl template.

Default The configuration does not have a default server-side SSH template.

Mode Global Configuration mode

Usage The normal form of this command creates a server-SSH configuration template.

The **no** form of this command removes the template.

You can bind only one server-SSH template to a virtual port. However, you can bind the same server-SSH template to multiple ports.

forward-proxy-enable

Description Enables SSH Insight support on ACOS SLB real server.

Syntax

```
[no] forward-proxy-enable
```

Default Not enabled.

Mode SLB server-SSH template

Example Enable this feature:

```
ACOS(config)#slb template server-ssh SSHInsight_ServerSide
ACOS(config-server ssh)#forward-proxy-enable
```

slb template ssli

Description Configures a virtual server template that specifies the accepted protocols that the virtual server can provide SSLi services. The `type` sub-commands specify the accepted protocols running over SSL.

Syntax

```
[no] slb template ssli template-name
```

Parameter	Description
template-name	Template name (1-127 characters)

This command enters the SLB SSLi Template Configuration Mode for the specified SSLi template.

Default SSLi on HTTPS sessions is enabled by default.

Mode Configuration mode

Example Create an SLB SSLi template for SMTP:

```
ACOS(config)# slb template ssli smtp_insight
ACOS(config-ssli)# type smtp
```

type

Description Specifies the service that is intercepted by SSLi.

Syntax `[no] type {http | xmpp | smtp | pop | ftp| ldap}`

Parameter	Description
http	HTTP service.
xmpp	XMPP service.
smtp	SMTP service.
pop	POP service.
ftp	FTP service.
ldap	LDAP service.

Default HTTP

Mode SLB SSLi template

Example Create an SLB SSLi template for SMTP:

```
ACOS(config)# slb template ssli ssli-tmp1
ACOS(config-ssli)# type smtp
```

debug ssl

Description Debug ssl operation.

Syntax **debug ssl { clientside | serverside | payload-dump-max** *<num>* **| payload-dump-string }**

Parameter	Description
clientside	Enables debugging for client-side SSL connections.

Parameter	Description
	Use this option to capture and analyze SSL traffic between the client and the Thunder device.
`serverside`	Enables debugging for server-side SSL connections. Use this option to capture and analyze SSL traffic between the Thunder device and the backend server.
`payload-dump-max` *<num>*	Specifies the maximum application payload size (in bytes) to be dumped for each SSL record. You can specify a value in the range of 0 to 2147483647. Setting the value as 0 disables payload dumping.
`payload-dump-string`	Enables dumping of application payload in string format.

Default N/A

Mode Enable Mode

Usage This command enables real-time debugging of SSL traffic on the Thunder device. It is useful for troubleshooting SSL handshakes, encryption or decryption issues, and inspecting payload data during SSL processing.

NOTE: Each **`debug ssl`** command overwrites the previous debug SSL settings.

Example The following command enables debugging for client-side SSL connections:

```
ACOS# debug ssl clientside
```

Example The following command enables debugging for server-side SSL connections:

```
ACOS# debug ssl serverside
```

Example The following command enables debugging for server-side SSL connections without dumping any payload data:

```
ACOS# debug ssl payload-dump-max 0 serverside
```

Example The following command enables debugging for client-side SSL connections and dumps up to 1024 bytes of payload data:

```
ACOS# debug ssl payload-dump-max 1024 clientside
```

web-category

Description Configure the operation of web category classification.

Syntax

```
[no] web-category
```

This command changes the CLI to configuration level for Web Category classification, where the following commands are available:

Command	Description
[no] **category-list category-list-name**	Create a list of web categories to provide criteria used in configuration forward-policy source destination rules. See the `destination` command under the `forward-policy` command. After entering the command, you are placed in a sub-configuration mode where predefined lists are specified to be part of the named category-list. The command **enable** for web-category must precede configuration of a category-list.
[no] **cloud-query-disable**	Disables cloud queries for URLs that are not present in the local cache or database. By default, cloud queries are enabled.
[no] **database-server** *server-url*	URL of the BrightCloud database server. Default: database.brightcloud.com

Command	Description
	NOTE: The **database-server** command is supported in the legacy Web Category SDK version 4.40.
[**no**] **db-update-time** *hh*:*mm*	Time of day at which ACOS requests an updated web category database from the BrightCloud server. Default is 00:00 (12 a.m.).
[**no**] **enable**	Initializes and enables the BrightCloud library. The web-category license file must be imported prior to using this feature to enable the feature. Disabled by default.
[**no**] **port** *portnum*	Protocol port where the BrightCloud server listens for requests. Default is 80. **NOTE:** The **port** command is supported in the legacy Web Category SDK version 4.40.
[**no**] **proxy-server**	Command in web-category configuration mode that specifies a proxy-server to use for querying the BrightCloud database server. This command places you in a sub-configuration mode, where the commands in web-category are available.
[**no**] remote-syslog-enable	Enables data plane logging to a remote syslog server.
[no] reputation-scope *scope-name*	Specify the scope of web reputation. The value can be greater-than or less-than the score level or customized score. And only one entry can be set in one scope for each greater-than or less-than

Command	Description
	setting. You can bind this setting to forward policy template for destination rule.
[no] **rtu-update-disable**	Disables realtime updates. Enabled by default. ACOS periodically checks for realtime updates based on the **rtu-update-interval** setting and adds them to the service cache.
[no] **rtu-update-interval** *minutes*	Interval at which to periodically check for real time updates. You can specify 10-14400 minutes. Default is 60 minutes.
[no] **server** *server-url*	URL of the BrightCloud server. Default: service.brightcloud.com
[no] **server-timeout** *seconds*	Maximum number of seconds to wait for BrightCloud server to respond to a query from ACOS. You can specify 1-300 seconds. If a reply is not received before the timeout, ACOS terminates the connection with the server. Default is 15 seconds.
[no] **ssl-port** *seconds*	Protocol port where the BrightCloud server listens for SSL traffic. Default is 443.
[no] **use-mgmt-port**	Uses the management interface for all communication with BrightCloud servers, including downloading the database and any lookup queries.

The `category-list-name` sub command contains the following categories.

Category list Name	Description
abortion	Category Abortion
adult-and-pornography	Category Adult and Pornography
alcohol-and-tobacco	Category Alcohol and Tobacco
auctions	Category Auctions
bot-nets	Category Bot Nets
business-and-economy	Category Business and Economy
cdns	Category CDNs
cheating	Category Cheating
computer-and-internet-info	Category Computer and Internet Info
computer-and-internet-security	Category Computer and Internet Security
confirmed-spam-sources	Category Confirmed SPAM Sources
cult-and-occult	Category Cult and Occult
dating	Category Dating
dead-sites	Category Dead Sites (db Ops only)
dns-over-https	Category DNS over HTTPs
drugs	Category Abused Drugs
dynamic-comment	Category Dynamic Comment
educational-institutions	Category Educational Institutions
entertainment-and-arts	Category Entertainment and Arts
fashion-and-beauty	Category Fashion and Beauty
financial-services	Category Financial Services
food-and-dining	Category Food and Dining
gambling	Category Gambling
games	Category Games
generative-ai	Category Generative AI

Category list Name	Description
government	Category Government
gross	Category Gross
hacking	Category Hacking
hate-and-racism	Category Hate and Racism
health-and-medicine	Category Health and Medicine
home-and-garden	Category Home and Garden
hunting-and-fishing	Category Hunting and Fishing
illegal	Category Illegal
illegal-pornography	Category Illegal Pornography eg. Child Sexual Abuse
image-and-video-search	Category Image and Video Search
internet-communications	Category Internet Communications
internet-portals	Category Internet Portals
job-search	Category Job Search
keyloggers-and-mon-itoring	Category Keyloggers and Monitoring
kids	Category Kids
legal	Category Legal
local-information	Category Local Information
low-thc-cannabis-products	Category Low THC Cannabis Products
malware-sites	Category Malware Sites
marijuana	Category Marijuana
military	Category Military
motor-vehicles	Category Motor Vehicles
music	Category Music
news-and-media	Category News and Media
nudity	Category Nudity

Category list Name	Description
nudity-artistic	Category Artistic Nudity
online-greeting-cards	Category Online Greeting cards
open-http-proxies	Category Open HTTP Proxies
parked-domains	Category Parked Domains
pay-to-surf	Category Pay to Surf
peer-to-peer	Category Peer to Peer
personal-sites-and-blogs	Category Personal sites and Blogs
personal-storage	Category Personal Storage
philosophy-and-politics	Category Philosophy and Political Advocacy
phishing-and-other-fraud	Category Phishing and Other Frauds
private-ip-addresses	Category Private IP Addresses
proxy-avoid-and-anonym-izers	Category Proxy Avoid and Anonym-izers
questionable	Category Questionable
real-estate	Category Real Estate
recreation-and-hobbies	Category Recreation and Hobbies
reference-and-research	Category Reference and Research
religion	Category Religion
search-engines	Category Search Engines
self-harm	Category Self Harm
sex-education	Category Sex Education
shareware-and-freeware	Category Shareware and Freeware
shopping	Category Shopping
social-network	Category Social Network
society	Category Society

Category list Name	Description
spam-urls	Category SPAM URLs
sports	Category Sports
spyware-and-adware	Category Spyware and Adware
stock-advice-and-tools	Category Stock Advice and Tools
streaming-media	Category Streaming Media
swimsuits-and-intimate-apparel	Category Swimsuits and Intimate Apparel
training-and-tools	Category Training and Tools
translation	Category Translation
travel	Category Travel
uncategorized	Uncategorized URLs
unconfirmed-spam-sources	Category Unconfirmed SPAM Sources
violence	Category Violence
weapons	Category Weapons
web-advertisements	Category Web Advertisements
web-based-email	Category Web based email
web-hosting-sites	Category Web Hosting Sites

The `proxy-server` commands places the device in web-category-proxy-server configuration mode.

Command	Description
`[no] proxy-host` *hostID*	Sub-command in web-category-proxy-server configuration mode to specify the proxy server's hostname or IP address to connect to. • *hostID* Proxy server's hostname or the proxy server's IP address in either IPv4 or IPv6 format.
`[no] http-`	Sub-command in web-category-proxy-server

Command	Description
`port port-num`	configuration mode to specify the proxy server port to connect to through HTTP protocol. • *port-num* Port number of the proxy server to connect to through HTTP protocol. If https-port is not configured, both HTTPS and HTTP communication will be handled through the configured HTTP port. **NOTE:** The **http-port** command is supported in the legacy Web Category SDK version 4.40.
`[no] https-port port-num`	Sub-command in web-category-proxy-server configuration mode to specify the proxy server port to connect to through HTTPS protocol. If no HTTPS port is specified, HTTP protocol will be used. *port-num* Port number of the proxy server to connect to through HTTPS protocol. If http-port is not configured, both HTTPS and HTTP communication will be handled through the configured HTTPS port.
`[no] username proxy-auth-username`	Sub-command in web-category-proxy-server configuration mode to specify the username to use for authentication when connecting with the proxy server. proxy-auth-username - Username to use for proxy server authentication.
`[no] password proxy-auth-password`	Sub-command in web-category-proxy-server configuration mode for specifying the password to use for authentication when connecting with proxy server.

Command	Description
	proxy-auth-password - Password to use for proxy server authentication.

`[no] auth-type {ntlm [domain ntlm-realm]| basic}`	Sub-command in web-category-proxy-server configuration mode to specify the authentication protocol type when connecting to proxy server. The following options are available in this command:
	`ntlm domain ntlm-realm`
	Specify NTLM authentication protocol. Specifying NTLM realm is optional.
	NTLM version 2 is used if this protocol is configured. NTLM version 1 is not supported.
	`basic`
	Specify BASIC authentication protocol.
	A username and password must be configured for the authentication protocol used.
	NOTE: The **`auth-type ntlm`** command is supported in the legacy Web Category SDK version 4.40.

Default N/A

Mode web-category configuration mode

Usage The web-category configuration defines actions related to URL classification and
configuration for connecting with the BrightCloud servers and is normally used in conjunction with **`forward-policy source`** rules that link destination and matching rules for an **`slb template policy`** through a category-list and specifying categories for bypassing traffic in the **`forward-proxy-bypass`** command in **`slb template client-ssl`** for SSLi configuration. The URLs are categorized in a third-party database

(BrightCloud) that ACOS can download and periodically pull down updates from.

Example Configure an ACOS device to use a proxy-server through NTLM authentication protocol to connect with BrightCloud servers.

```
ACOS(config)# web-category
ACOS(config-web-category)# proxy-server
ACOS(config-web-category-proxy-server)# proxy-host 192.0.2.0
ACOS(config-web-category-proxy-server)# http-port 3128
ACOS(config-web-category-proxy-server)# https-port 8080
ACOS(config-web-category-proxy-server)# auth-type ntlm domain
example
ACOS(config-web-category-proxy-server)# username exampleadmin
ACOS(config-web-category-proxy-server)# password
0e1x2a3m4p5l6e7
ACOS(config-web-category-proxy-server)# exit
```

Example Configure the web-category list `Mail_Categories`, then apply that list to the configuration of the forward-policy source list `Any_Source`. Any request whose destination is in the `Web_Mail_List` web-category-list is forwarded.

```
ACOS(config)# web-category
ACOS(config-web-category)# enable
Please check the show log output for Web category enable
status
ACOS(config-web-category)# category-list Web_Mail_List
ACOS(config-web-category-category-list)# web-based-email
ACOS(config-web-category-category-list)# exit
ACOS(config-web-category)# exit
ACOS(config)#
...
ACOS(config-policy-forward-policy)# source Any_Source
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination web-
category-list Web_Mail_List action ForwardMail
```

Example Enable web category classification, then apply web-category classification to bypass SSLi decryption and inspection for websites classified as category-list.

```
ACOS(config)# web-category
ACOS(config-web-category)# enable
ACOS(config-web-category)# exit
ACOS(config)#
...
ACOS-Inside(config)# slb template client-ssl SSLInsight_
ClientSide
ACOS-Inside(config-client ssl)# forward-proxy-bypass web-
category financial-services
ACOS-Inside(config-client ssl)# forward-proxy-bypass web-
category educational-institutions
ACOS-Inside(config-client ssl)# forward-proxy-bypass web-
category health-and-medicine
ACOS-Inside(config-client ssl)# forward-proxy-bypass
exception-web-category low-thc-cannabis-products
ACOS-Inside(config-client ssl)# forward-proxy-bypass
exception-web-category generative-ai
ACOS-Inside(config-client ssl)# forward-proxy-bypass
exception-web-category dns-over-https
```

Show Commands

show slb ssl

Description Show SSL statistics.

For the Multi-PU platforms, the statistics will display the aggregated counters; PU1 + PU2.

Syntax

```
show slb ssl {error | module-usage | processing-unit | stats
| thales-hsm}
```

Parameter	Description
error	Shows errors such as cookie mismatch, wrong signature length, unsupported cipher,

Parameter	Description
	incorrect public key, no certificate returned, etc.
module-usage	Shows the SSL hardware module usage (PU1 or PU2). This option is available only on Multi-PU platform.
processing-unit {ID <1-2>}	Shows the statistic of the specific processing-unit (PU1 or PU2). This option is available only on Multi-PU platform.
stats	Shows statistics for SSL modules.
thales-hsm {counters | logs | statistics | status}	Shows the counters, logs, statistics, and status for Thales SSL Hardware Security Module (HSM) device. **NOTE:** Thales HSM is not supported on all new SSL modules.

Mode All

Example The following command shows SSL SLB statistics:

```
ACOS# show slb ssl stats
SSL module: Hardware
Number of SSL modules: 1
SSL module 1
    number of enabled crypto engines: 8
    number of available crypto engines: 8
    number of requests handled: 0
    Current clientside SSL connections: 0
    Total clientside SSL connections: 0
    Current serverside SSL connections: 0
    Total serverside SSL connections: 0
    Total Non SSL Bypass connections: 0
    Total times of reusing SSL sessions(IDs) in client ssl 0
    Total times of reusing SSL sessions(IDs) in server ssl 0
```

```
Failed SSL handshakes: 0
    Failed crypto operations: 0
    SSL memory usage: 8132 bytes
    SSL server certificate errors: 0
    SSL client certificate authorization failed: 0
    SSL fail CA verification 0
    HW Context Memory Total Count 497102
    HW Context Memory in Use 0
    HW Context Memory alloc failed 0
    HW ring full 0
    Record too big 0
    Total client ssl context malloc failures: 0
    Maximum SSL contexts 8256
    Current SSL contexts in use 0
    Static SSL contexts in use 0
    Dynamic SSL contexts in use 0
SSL Forward Proxy
    Bypass Failsafe SSL sessions: 0
    Bypass SNI sessions: 0
   Bypass ESNI sessions: 3
    Bypass Client Auth sessions: 0
    Failed in SSL handshakes: 0
    Failed in crypto operations: 0
    Failed in TCP: 0
    Failed in Certificate verification: 0
    Failed in Certificate signing: 0
    Invalid OCSP Stapling Response: 0
    Revoked OCSP Response: 0
    Unsupported SSL version: 0
SSLi Errors
    Cert fetch, Fatal alert: 0
    Cert fetch, TCP FIN/RST: 0
    Cert fetch, validation error: 0
    Client SSL, Fatal Alert: 0
    Client SSL, TCP FIN/RST, Pinning: 0
    Client SSL, Internal error: 0
    Client SSL, Unknown error: 0
    SSL Session, TCP FIN/RST: 0
    Server SSL, Fatal alert: 0
    Server SSL, TCP FIN/RST: 0
```

```
    Server SSL, Internal error: 0
    Server SSL, Unknown error: 0
```

The following table describes the fields on this output.

Field	Description
SSL Module	"Hardware" indicates SSL processing occurs in hardware modules. "Software" indicates SSL processing occurs in ACOS software.
Number of SSL modules	Total number of SSL processing modules on the ACOS device.
SSL module *n*	ID number of the SSL module to which the following statistics apply.
number of enabled crypto engines	Number of SSL encryption/decryption processing engines that are enabled.
number of available crypto engines	Number of SSL encryption/decryption processing engines that are available on the device.
number of requests handled	Number of SSL requests handled by the SSL processing engine.
Current clientside SSL connections	Number of currently active SSL client-side SSL sessions (sessions between ACOS and clients).
Total clientside SSL connections	Total number of SSL client-side sessions since the last time statistics were cleared.
Current serverside SSL connections	Number of currently active SSL server-side SSL sessions (sessions between ACOS and servers).
Total serverside SSL connections	Total number of SSL server-side sessions since the last time statistics were cleared.
Total times of	SSL session-ID reuse statistics.

Field	Description
reusing SSL sessions(IDs) in client ssl	
Total times of reusing SSL sessions(IDs) in server ssl	
Failed SSL handshakes	Number of SSL sessions in which the SSL security handshake failed.
Failed crypto operations	Number of times an encryption/decryption failure occurred for an SSL record.
Dropped serverside SSL connections	Total number of SSL server-side sessions dropped since the last time statistics were cleared.
SSL memory usage	Amount of memory in use by the SSL processing module.
SSL server certificate errors	Total count of certificate errors.
SSL fail CA verification	Number of times an SSL session was terminated due to a certificate verification failure.
HW Context Memory Total Count	Total amount of hardware available for SSL context memory allocation.
HW Context Memory in Use	Total amount of hardware in use for SSL context memory allocation.
HW Context Memory alloc failed	Number of times the encryption processor was unable to allocate memory.
HW ring full	Number of times the ACOS software was unable to enqueue an SSL record to the SSL processor for encryption/decryption. (Number of times the

Field	Description
	processor reached its performance limit.)
Record too big	Number of times the ACOS device received an SSL record that spanned across more than 64 packets.
Total client ssl context malloc failures	Number of times ACOS failed to allocate memory for client SSL context memory.
Bypass Failsafe SSL sessions	Number of bypassed SSL sessions
Bypass SNI sessions	Number of bypassed SSL sessions based on SNI criteria specified in the ACOS configuration.
Bypass ESNI sessions	Number of bypassed SSL sessions based on ESNI criteria specified in the ACOS configuration.
Bypass Client Auth sessions	Number of bypassed SSL sessions based on client authentic criteria specified in the ACOS configuration.
Failed in SSL handshakes	Number of SSL sessions in which the SSL security handshake failed.
Failed in crypto operations	Number of times an encryption/decryption failure occurred for an SSL record.
Failed in TCP	Number of TCP sessions that failed.
Failed in Certificate verification	Number of SSL sessions in which the SSL security handshake failed.
Failed in Certificate signing	Number of times an SSL session was terminated due to a certificate verification failure.
Invalid OCSP Stapling Response	Number of times an SSL session was terminated due to a certificate verification failure message in the OCSP stapling response.
Revoked OCSP	Number of times an SSL session was terminated

Field	Description
Response	due to a certificate verification failure message in the OCSP response.

NOTE: The description of SSLi error counter fields is similar to the description of the SSLi inspection failure error logs. For more information, see the *SSLi Configuration Guide*.

Example The following command shows SSL SLB statistics for Multi-PU platform:

```
ACOS# show slb ssl stats
```

```
SSL module: QAT
Config module: Hardware
Number of SSL modules: 18
PU1 SSL module 1
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 28
PU1 SSL module 2
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 23
PU1 SSL module 3
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 23
PU1 SSL module 4
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 27
PU1 SSL module 5
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 18
PU1 SSL module 6
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 25
PU1 SSL module 7
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 0
PU1 SSL module 8
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 0
PU1 SSL module 9
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
```

```
    Number of requests handled: 0
PU2 SSL module 1
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 13
PU2 SSL module 2
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 16
PU2 SSL module 3
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 15
PU2 SSL module 4
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 14
PU2 SSL module 5
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 15
PU2 SSL module 6
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 17
PU2 SSL module 7
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 16
PU2 SSL module 8
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 11
PU2 SSL module 9
    Number of enabled crypto engines: 48
    Number of available crypto engines: 64
    Number of requests handled: 11
    Current clientside SSL connections: 0
```

```
    Total clientside SSL connections: 19
    Current serverside SSL connections: 0
    Total serverside SSL connections: 34
    Total Non SSL Bypass connections: 0
    Total times of stateful session reuse in client ssl: 0
    Total times of stateful session reuse in server ssl: 0
    Total times of stateless session reuse in client ssl: 0
    Total times of stateless session reuse in server ssl: 0
    Total clientside early data connections: 0
    Total serverside early data connections: 0
    Total clientside failed early data connections: 0
    Total serverside failed early data connections: 0
    Failed SSL handshakes: 0
    Failed crypto operations: 0
    SSL memory usage: 778804 bytes
    SSL server certificate errors: 0
    SSL client certificate authorization failed: 0
    SSL fail CA verification 0
    HW Context Memory alloc failed 0
    HW ring full 0
    Record too big 0
    Total client ssl context malloc failures: 0
    Maximum SSL contexts N/A
    Current SSL contexts in use 4
    Static SSL contexts in use 4
    Dynamic SSL contexts in use 0
SSL Forward Proxy
    Bypass Failsafe SSL sessions: 0
    Bypass Username sessions: 0
    Bypass AD-Group sessions: 0
    Bypass SNI sessions: 0
    Bypass Certificate subject sessions: 0
    Bypass Certificate issuer sessions: 0
    Bypass Certificate SAN sessions: 0
    Bypass NO SNI sessions: 0
    Reset NO SNI sessions: 0
    Bypass ESNI sessions: 0
    Drop ESNI sessions: 0
```

```
    Bypass Client Auth sessions: 0
    Failed in SSL handshakes: 0
    Failed in crypto operations: 0
    Failed in TCP: 0
    Failed in Certificate verification: 0
    Failed in Certificate signing: 0
    Invalid OCSP Stapling Response: 0
    Revoked OCSP Response: 0
    Unsupported SSL version: 0
    Bypass triggered by aFleX: 0
SSLi Errors
    Cert fetch, Fatal alert: 0
    Cert fetch, TCP FIN/RST: 0
    Cert fetch, validation error: 0
    Client SSL, Fatal Alert: 0
    Client SSL, TCP FIN/RST, Pinning: 0
    Client SSL, Internal error: 0
    Client SSL, Unknown error: 0
    SSL Session, TCP FIN/RST: 0
    Server SSL, Fatal alert: 0
    Server SSL, TCP FIN/RST: 0
    Server SSL, Internal error: 0
    Server SSL, Unknown error: 0
```

Example

The `show slb ssl stats` command provides information about optimizing QAT mapping. If the SSL VF and vCPU count for the VM are suboptimal, recommendations will appear in pink. The tags next to the SSL module number indicate its status:

- [Partial] - The module is not fully utilized.
- [Disabled] - The module is disabled and inactive.

NOTE:

The changes only apply to the vThunder in Next Gen Multi-tenant Virtual Platform (MVP) with QAT4 SSL VF.

The following output shows SSL SLB statistics for a vThunder with 13 data CPU and 8 QAT VF:

```
ACOS# show slb ssl stats
SSL module: QAT
```

```
Config module: Hardware
Number of SSL modules: 8
     But only 7 enabled to align with the data CPU Consider
adding 3 more data CPU
     Or remove 1 SSL module for optimize performance
SSL module 1
    Number of enabled crypto engines: 4
    Number of available crypto engines: 4
    Number of requests handled: 64980
SSL module 2
    Number of enabled crypto engines: 4
    Number of available crypto engines: 4
    Number of requests handled: 64675
SSL module 3
    Number of enabled crypto engines: 4
    Number of available crypto engines: 4
    Number of requests handled: 65028
SSL module 4
    Number of enabled crypto engines: 4
    Number of available crypto engines: 4
    Number of requests handled: 64822
SSL module 5
    Number of enabled crypto engines: 4
    Number of available crypto engines: 4
    Number of requests handled: 64364
SSL module 6
    Number of enabled crypto engines: 4
    Number of available crypto engines: 4
    Number of requests handled: 65109
SSL module 7 [Partial]
    Number of enabled crypto engines: 2
    Number of available crypto engines: 4
    Number of requests handled: 32398
SSL module 8 [Disabled]
    Number of enabled crypto engines: 0
    Number of available crypto engines: 4
    Number of requests handled: 0
```

show slb ssl-cert-revoke-stats

Description Show statistics for certificate revocation check.

For the Multi-PU platforms, the statistics displays the aggregated counters; PU1 + PU2.

Syntax

```
show slb ssl-cert-revoke-stats
```

Example

```
ACOS# show slb ssl-cert-revoke-stats
OCSP stapling response good:          0
Certificate chain status good:        0
Certificate chain status revoked:     0
Certificate chain status unknown:     0
OCSP requests:                        0
OCSP responses:                       0
OCSP connection errors:               0
OCSP URI not found:                   0
OCSP URI https:                       0
OCSP URI unsupported:                 0
OCSP response status good:            0
OCSP response status revoked:         0
OCSP response status unknown:         0
OCSP cache status good:               0
OCSP cache status revoked:            0
OCSP cache miss:                      0
OCSP cache expired:                   0
OCSP other errors:                    0
CRL requests:                         0
CRL responses:                        0
CRL connection errors:                0
CRL URI not found:                    0
CRL URI https:                        0
CRL URI unsupported:                  0
CRL response status good:             0
CRL response status revoked:          0
CRL response status unknown:          0
CRL cache status good:                0
CRL cache status revoked:             0
CRL other errors:                     0
```

The following table describes the fields on this output.

Field	Description
OCSP stapling response good	Number of times the OCSP stapling response was good.

Field	Description
Certificate chain status good	Number of times the certificate chain status was good.
Certificate chain status revoked	Number of times the certificate chain status was revoked.
Certificate chain status unknown	Number of times the certificate chain status was unknown.
OCSP requests	Number of OCSP requests.
OCSP responses	Number of OCSP responses.
OCSP connection errors	Number of OCSP connection errors.
OCSP URI not found	Number of times the OCSP URI was not found.
OCSP URI https	Number of times the OCSP URI was HTTPS.
OCSP URI unsupported	Number of times the OCSP URI was unsupported.
OCSP response status good	Number of times the OCSP response status was good.
OCSP response status revoked	Number of times the OCSP response status was revoked.
OCSP response status unknown	Number of times the OCSP response status was unknown.
OCSP cache status good	Number of times the OCSP cache status was good.
OCSP cache status revoked	Number of times the OCSP cache status was revoked.
OCSP cache miss	Number of times the OCSP cache was missed.
OCSP cache expired	Number of times the OCSP cache was expired.
OCSP other errors	Number of times OCSP had other errors.

Field	Description
CRL requests	Number of CRL requests.
CRL responses	Number of CRL responses.
CRL connection errors	Number of CRL connection errors.
CRL URI not found	Number of times the CRL URI was not found.
CRL URI https	Number of times the CRL URI was HTTPS.
CRL URI unsupported	Number of times the CRL URI was unsupported.
CRL response status good	Number of times the CRL response status was good.
CRL response status revoked	Number of times the CRL response status was revoked.
CRL response status unknown	Number of times the CRL response status was unknown.
CRL cache status good	Number of times the CRL cache status was good.
CRL cache status revoked	Number of times the CRL cache status was revoked.
CRL other errors	Number of times CRL had other errors.

show slb ssl-counters

Description Shows the number of successes and failures for key exchange methods, and SSL/TLS version. Shows the session cache count for new, hits, missed, and expired. Shows the average handshake time and total renegotiations.

Syntax

```
show slb ssl-counters [vserver [vport]]
```

Field	Description
vserver	Specifies virtual server name. 1 to 127 characters.
vport	Specifies virtual port ID. Integer from 0 to 65534. No default value.

Example

In this example, the TPS device is configured with two virtual servers, `vip1` and `vip2`, each of which is bound to two virtual ports each, `443` and `444`.

The statistics of vip1, port 443

```
ACOS# sh slb ssl-counters vip1 443
Virtual Server Name: vip1 Port: 443
------------------------------------------------------------
------------------
Cumulative sessions = 4

ID            Name                                Successes
Failures
0x0300002f      TLS1_RSA_AES_128_SHA                  1
 0
0x0300003d      TLS1_RSA_AES_256_SHA256               3
 0

Key Exchange Methods                              Successes
Failures
  RSA
    1024 bits                                         4
 0
  ECDHE
  DHE

SSL/TLS Version                                   Successes
Failures
TLS1.1                                                1
 0
TLS1.2                                                3
 0

Session Cache                                     Count
New                                                   4
Hit                                                   0
Miss                                                  0
Expired                                               0
```

```
Handshake Average time = 7 ms

Renegotiation Counters
Total renegotiations = 0

Renegotiated SSL/TLS Versions                    Successes
Failures
(none used)
```

The statistics of vip1, port 444

```
ACOS# sh slb ssl-counters vip1 444
Virtual Server Name: vip1 Port: 444
------------------------------------------------------------------
------------------
Cumulative sessions = 3

ID              Name                             Successes
Failures
0x0300000a      SSL3_RSA_DES_192_CBC3_SHA           1
  0
0x0300009d      TLS1_RSA_AES_256_GCM_SHA384         2
  0

Key Exchange Methods                             Successes
Failures
  RSA
    2048 bits                                        3
  0
  ECDHE
  DHE

SSL/TLS Version                                  Successes
Failures
SSLv3                                               1
  0
TLS1.2                                              2
  0
```

```
Session Cache                                          Count
New                                                      3
Hit                                                      0
Miss                                                     0
Expired                                                  0

Handshake Average time = 10 ms

Renegotiation Counters
Total renegotiations = 0

Renegotiated SSL/TLS Versions                          Successes
Failures
(none used)
```

This “show slb ssl-counters” command output displays statistics for TLS 1.3 cipher. Add new counter for TLS1.3 cipher. Add new counter for version downgrade(1.3 to 1.2)

```
ACOS# show slb ssl-counters vip1
Virtual Server Name: vip1
------------------------------------------------------------------
----------
Client ssl stats
Cumulative sessions = 0

ID         Name                                        Successes
Failures
0x0300c030 TLS1_ECDHE_RSA_AES_256_GCM_SHA384           2
0
0x03001301 TLS13_AES_128_GCM_SHA256                    1
0
0x03001302 TLS13_AES_256_GCM_SHA384                    6
0
0x03001303 TLS13_CHACHA20_POLY1305_SHA256              3
0

Key Exchange Methods                                   Successes
Failures
  RSA
  ECDHE
```

```
  DHE

SSL/TLS Version                                    Successes
Failures
TLS1.2                                             2
0

TLS1.3                                             10
0
```

The statistics of SNI bypass due to missing cert/key

```
ACOS# sh slb ssl-counters ep_in_vs
Virtual Server Name: ep_in_vs
-------------------------------------------------------------------
------------------
Client ssl stats
Cumulative sessions = 1

ID          Name                                   Successes
Failures
(none used)

Key Exchange Methods                               Successes
Failures
RSA
ECDHE
DHE
SSL/TLS Version                                    Successes
Failures
(none used)

Session Cache                                      Count
New                                                1
Hit                                                0
Miss                                               0
Expired                                            0
Current                                            0

Handshake Average time = 0 ms
```

```
Handshake Failures = 0

Certificate Auth = 0
SNI Auto-Map Successes = 0
SNI Auto-Map Failures = 0
SNI Auto-Map Failures Connection Closed = 0
SNI Auto-Map Failures Max Active Connections = 0
SNI Auto-Map Failures Missing Cert/Key = 0
SNI Bypass due to Missing Cert/Key = 1
SNI Bypass due to Certificate Expired = 0
SNI Bypass due to Matched Explicit Bypass List = 0

Renegotiation Counters
Total renegotiations = 0

Renegotiated SSL/TLS Versions                    Successes
Failures
(none used)
```

Example The following command shows the SSL statistics of PU1 in the Multi-PU platforms, which shows the aggregated counters; PU1 + PU2:

NOTE: Some of the operational command statistics are displayed separately. For example, the 'Average Handshake Time' will display the PU1 and PU2 statistics separately: `Handshake Average time: PU1:209ms PU2:217ms.`

```
On Primary Processing Unit:
-----------------------------------------------------------------
--
ACOS(config)#show slb ssl-counters
Global Stats
-----------------------------------------------------------------
------------------
Client ssl stats
Cumulative sessions = 1578

ID         Name                                  Successes
Failures
0x03000035 TLS1_RSA_AES_256_SHA                  1578
```

```
0

Key Exchange Methods                                Successes
Failures
  RSA
    1024 bits                                       1578
0
  ECDHE
  DHE

SSL/TLS Version                                     Successes
Failures
TLS1.0                                              1578
0


Session Cache                                       Count
New                                                 1578
Hit                                                 0
Miss                                                0
Expired                                             0
Current                                             0

Handshake Average time: PU1:2ms PU2:19ms
Handshake Failures = 0
Certificate Auth = 0
SNI Auto-Map Successes = 0
SNI Auto-Map Failures = 0
SNI Auto-Map Failures Connection Closed = 0
SNI Auto-Map Failures Max Active Connections = 0
SNI Auto-Map Failures Missing Cert/Key = 0
SNI Bypass due to Missing Cert/Key = 0
SNI Bypass due to Certificate Expired = 0
SNI Bypass due to Matched Explicit Bypass List = 0

Renegotiation Counters
Total renegotiations = 0
```

```
Renegotiated SSL/TLS Versions                       Successes
Failures
(none used)

Global Stats
------------------------------------------------------------------
------------------
Server ssl stats
Cumulative sessions = 5

ID          Name                                    Successes
Failures
0x0300c02b TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256  1
0
0x0300cca9 TLS1_ECDHE_ECDSA_CHACHA20_POLY1305_SHA256 4
    0

Key Exchange Methods                                Successes
Failures
  RSA
  ECDHE
    prime256v1                                      5
0
  DHE

SSL/TLS Version                                     Successes
Failures
TLS1.2                                              5
0


Session Cache                                       Count
New                                                 5
Hit                                                 0
Miss                                                0
Expired                                             0
Current                                             0

Handshake Average time: PU1:41ms PU2:37ms
```

```
Handshake Failures = 0
Certificate Auth = 0

Renegotiation Counters
Total renegotiations = 0

Renegotiated SSL/TLS Versions                    Successes
Failures
(none used)
```

Example The following command shows the SSL SLB statistics of PU2 in the Multi-PU platforms:

```
On Secondary Processing Unit:
------------------------------------------------------------------
--
ACOS#show slb ssl-counters
Global Stats
------------------------------------------------------------------
------------------
Client ssl stats
Cumulative sessions = 6

ID         Name                                  Successes
Failures
0x03000035 TLS1_RSA_AES_256_SHA                  6
0

Key Exchange Methods                             Successes
Failures
  RSA
    1024 bits                                    6
0
  ECDHE
  DHE

SSL/TLS Version                                  Successes
Failures
TLS1.0                                           6
```

```
0


Session Cache                                       Count
New                                                 6
Hit                                                 0
Miss                                                0
Expired                                             0
Current                                             0
Handshake Average time = 19 ms
Handshake Failures = 0
Certificate Auth = 0
SNI Auto-Map Successes = 0
SNI Auto-Map Failures = 0
SNI Auto-Map Failures Connection Closed = 0
SNI Auto-Map Failures Max Active Connections = 0
SNI Auto-Map Failures Missing Cert/Key = 0
SNI Bypass due to Missing Cert/Key = 0
SNI Bypass due to Certificate Expired = 0
SNI Bypass due to Matched Explicit Bypass List = 0

Renegotiation Counters
Total renegotiations = 0

Renegotiated SSL/TLS Versions                       Successes
Failures
(none used)

Global Stats
------------------------------------------------------------------
------------------
Server ssl stats
Cumulative sessions = 2

ID          Name                                    Successes
Failures
0x0300cca9 TLS1_ECDHE_ECDSA_CHACHA20_POLY1305_SHA256 2
    0
```

```
Key Exchange Methods                                Successes
Failures
  RSA
  ECDHE
    prime256v1                                      2
0
  DHE

SSL/TLS Version                                     Successes
Failures
TLS1.2                                              2
0


Session Cache                                       Count
New                                                 2
Hit                                                 0
Miss                                                0
Expired                                             0
Current                                             0
Handshake Average time = 37 ms
Handshake Failures = 0
Certificate Auth = 0

Renegotiation Counters
Total renegotiations = 0

Renegotiated SSL/TLS Versions                       Successes
Failures
(none used)
```

show slb ssl-crl

Description Show the retrieved Certificate Revocation List for a specific virtual port. If the certificate issuers have listed expiration dates for the certificates,

then this command will show you the issuer and the expired or not expired status

Syntax

```
show slb ssl-crl  vserver vport
```

Example

```
ACOS# show slb ssl-crl vip1 443
Virtual server(vipw : 443):

----Retrieved CRL----
Issuer: /C=FR/O=Certplus/CN=Class 2 Primary CA
Status: Not expired

Issuer: /OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
Status: Expired

Issuer: /CN=ComSign Secured CA/O=ComSign/C=IL
Status: Expired

Issuer: /C=US/O=Network Solutions L.L.C./CN=Network Solutions
Certificate Authority
Status: Expired

Issuer: /C=US/O=SecureTrust Corporation/CN=Secure Global CA
Status: Expired

Issuer: /C=US/O=SecureTrust Corporation/CN=SecureTrust CA
Status: Expired

Issuer: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig
Status: Expired

Issuer: /C=EU/O=AC Camerfirma SA CIF
A82743287/OU=http://www.chambersign.org/CN=Chambers of
Commerce Root
Status: Expired

Issuer: /CN=ACCVRAIZ1/OU=PKIACCV/O=ACCV/C=ES
Status: Expired
```

```
Issuer: /C=EU/O=AC Camerfirma SA CIF
A82743287/OU=http://www.chambersign.org/CN=Global Chambersign
Root
Status: Expired

Issuer: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate
Signing/CN=StartCom Certification Authority
Status: Expired

Issuer: /C=DE/O=TC TrustCenter GmbH/OU=TC TrustCenter Class 2
CA/CN=TC TrustCenter Class 2 CA II
Status: Not expired

Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA
Limited/CN=AAA Certificate Services
Status: Expired

Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA
Limited/CN=Secure Certificate Services
Status: Expired

Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA
Limited/CN=COMODO Certification Authority
Status: Expired

Issuer: /C=HU/L=Budapest/O=Microsec Ltd./OU=e-Szigno
CA/CN=Microsec e-Szigno Root CA
Status: Expired

Issuer: /CN=Autoridad de Certificacion Raiz del Estado
Venezolano/C=VE/L=Caracas/ST=Distrito Capital/O=Sistema
Nacional de Certificacion Electronica/OU=Superintendencia de
Servicios de Certificacion
Electronica/emailAddress=acraiz@suscerte.gob.ve
Status: Not expired

----End of CRL----

17 CRL retrieved
```

Example The following example displays the certification information from Multi-PU platforms. The CRL records of both the PUs are merged.

```
ACOS#show slb ssl-crl test 443
 Virtual server (test: 443):

----Retrieved CRL----
Issuer: fake issuer ASSL-0
Status: Expired
Processing Unit: 1
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-1
Status: Not expired
Processing Unit: 1
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-2
Status: Expired
Processing Unit: 1
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-3
Status: Not expired
Processing Unit: 1
----End of CRL----
.
.
.
----Retrieved CRL----
Issuer: fake issuer ASSL-205
Status: Not expired
Processing Unit: 2
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-206
Status: Expired
```

```
Processing Unit: 2
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-207
Status: Not expired
Processing Unit: 2
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-208
Status: Expired
Processing Unit: 2
----End of CRL----

----Retrieved CRL----
Issuer: fake issuer ASSL-209
Status: Not expired
Processing Unit: 2
----End of CRL----

 420 CRL retrieved
```

show slb ssl-cert-pinning-candidate-list

Description Show or clear certificate pinning candidate list (in descending order of counters).

Syntax

```
show slb ssl-cert-pinning-candidate-list num {alphabet-order | bypassed | local-list | central-list}

clear slb ssl-cert-pinning-candidate-list {server-name} <1-255 characters>
```

Mode All

Example The following show command output displays the candidate list:

```
ACOS(config)# show slb ssl-cert-pinning-candidate-list
SNI                    Counter          TTL
-----------------------------------------------
```

```
youtube.com              10              1440
gmail.com                6               1440
google.com               5               1440
yahoo.com                3               1440
api.snapcraft.io         1               1430
```

The following table describes the fields in the show command output:

Field	Description
SNI	List of Server Name Indication or Destination domain.
Counter	The number of times cert-pinning occurred.
TTL	Time-to-Live (TTL) value.

Example The following show command output displays the central candidate list in alphabetical order:

```
ACOS#show slb ssl-cert-pinning-candidate-list central-list
alphabet-order
Central Updated Cert-Pinning Candidate List: (Total entries:
18)
SNI                                                Bypass count
a10networks.com                                    121
apple.com                                          183
apple12eu.com                                      11
arc.msn.com                                        163
citysports.com                                     192
client.dropbox.com                                 53
d.dropbox.com                                      1
dl-debug.dropbox.com                               50
dmap.com                                           11
gmail.com                                          106
google.com                                         111
humtv.com                                          198
iesco.com                                          127
nokia.com                                          200
store-images.s-microsoft.com                       86
storeedgefd.dsx.mp.microsoft.com                   167
tw.iherb.com.com                                   157
yahoo.com                                          194
```

Example The following show command output displays the local candidate list for Multi-PU platforms, which shows the PU1 and PU2 merged/integrated counters. However, the **total entries** will be the aggregated value; (PU1+PU2):

```
ACOS#show slb ssl-cert-pinning-candidate-list local-list
Local Generated Cert-Pinning Candidate List: (Total entries:
50)
SNI             PU   Conn failures  Bypass count   TTL(min)
www.gmail.com   1     70            20             1200
www.yahoo.com   1     56            37             1350
www.google.com  2     22            10             860
youtube.com     1     10             5             1440
gmail.com       1      7            50             1220
www.yahoo.com   2      5            10             1400
```

Limitation For local certificate pinning list in Multi-PU platforms:

- The connection failure counters are refreshed every second. As a result, if certificate pinning occurs more than once per second, the SSLi bypass trigger may be delayed if the number of connection failures exceeds the threshold. For example, if the SSLi bypass criteria of the connection failure is greater than 5, and the certificate pinning occurs three times within 1 second when the count is already four, then the first bypass case will be the eighth fail case.
- The local certificate pinning list varies between PU1 and PU2. This is because the SNI of the received requests is recorded and may contain different traffic for each PU.
- The number of displayed entries <display_number> may exceed the default value (8000) as both PU1 and PU2 entries are displayed simultaneously.

show slb ssl-cert-pinning-candidate-list central-list

Description Show the central certificate pinning candidate list.

Syntax

```
show slb ssl-cert-pinning-candidate-list {central-list <1-100>
| bypassed <1-100>| alphabet-order}
```

```
clear slb ssl-cert-pinning-candidate-list {central-list | SNI_
name | stats-only}
```

Parameter	Description
Show Command Options	
central-list	Show the centrally updated cert-pinning-candidate-list entries in descending order of bypass count.
bypassed	Show the bypassed entries that are defined in the client-SSL template bypassed rule set.
alphabet-order	Show the entries in the alphabetical order.
Clear Command Options	
SNI_name	Clear the specific SNI in local cert pinning list.
central-list	Clear the entire local cert pinning list.
stats-only	Clear the statistics only.

Mode All

Example The following example shows the command output with all the above options enabled:

```
ACOS(config)# show slb ssl-cert-pinning-candidate-list
central-list bypassed alphabet-order
Central Updated Cert-Pinning Candidate List:
SNI                      Bypass count
---------------------------------------
dashboard.snapcraft.io      501
odrs.gnome.org              300
api.snapcraft.io            113
cdn.fwupd.org               100
extensions.gnome.org        96
a10networks.com              0
```

Example The following show command output displays the central candidate list for Multi-PU platforms, which shows the aggregated bypassed time for each entry. The list in both the PUs is the same, and the maximum number of entries is 100:

```
ACOS#show slb ssl-cert-pinning-candidate-list central-list
Central Updated Cert-Pinning Candidate List: (Total entries:
18)
SNI                                  Bypass count
dl-debug.dropbox.com                 331
humtv.com                            291
yahoo.com                            273
client.dropbox.com                   261
gmail.com                            244
apple.com                            205
storeedgefd.dsx.mp.microsoft.com     194
d.dropbox.com                        193
citysports.com                       184
iesco.com                            172
tw.iherb.com.com                     169
google.com                           165
nokia.com                            154
arc.msn.com                          150
store-images.s-microsoft.com         112
a10networks.com                      40
apple12eu.com                        0
dmap.com                             0
```

The following table describes the fields in the show command output.

Field	Description
SNI	List of Server Name Indication or Destination domain.
Bypass Count	List of bypassed count.

show slb ssl-cert-pinning-candidate-list local-list

Description Show or clear the statistics of local cert pinning list.

Syntax

```
show slb ssl-cert-pinning-candidate-list {local-list <1-8000>
| bypassed <1-8000>| alphabet-order <1-8000>}

clear slb ssl-cert-pinning-candidate-list {local-list | SNI_
name | stats-only}
```

Parameter	Description
Show Command Options	
local-list	Show the locally generated cert-pinning-candidate-list entries. The range of the entries can be between 1-8000. By default, the value is 8000.
bypassed	Show the bypassed entries that are defined in the client-SSL template bypassed rule set. The range of the entries can be between 1-8000. By default, the value is 8000.
alphabet-order	Show the entries in the alphabetical order. The range of the entries can be between 1-8000. By default, the value is 8000.
Clear Command Options	
SNI_name	Clear the specific SNI in local cert pinning list.
local-list	Clear the entire local cert pinning list.
stats-only	Clear the statistics only.

Mode All

Example The following example shows the command output with all the above options enabled:

```
ACOS(config)# show slb ssl-cert-pinning-candidate-list local-
list bypassed alphabet-order
Local Generated Cert-Pinning Candidate List:
SNI                  Conn failures  Bypass count   TTL
-------------------------------------------------------------
api.snapcraft.io       501            60           60
cdn.fwupd.org          100            50           1100
dashboard.snapcraft.io 1200           56           930
extensions.gnome.org   100            73           1400
odrs.gnome.org         765            12           1010
```

The following table describes the fields in the show command output.

Field	Description
SNI	List of Server Name Indication or Destination domain.
Conn failures	List of connection failure count.
Bypass Count	List of bypassed count.
TTL	List of Time-to-Live (TTL) value.

show slb ssl-expire-check

Description Display information about email notification of expired certificates.

Syntax

```
show slb ssl-expire-check
```

Mode All

show slb ssl-forward-proxy-cert

Description Display hash entries for server certificates forged by ACOS device for SSLi. Also, display status of the forward-proxy-cert process. The `state` field displays whether the server certificate is being verified, whether a CA certificate is in the process of being forged, whether the ACOS software is ready to forge a new CA certificate, or whether ACOS software is in the ready state.

Syntax

```
show slb ssl-forward-proxy-cert name num {ipaddr | all} [sni]
```

Parameter	Description
name	Wildcard VIP name.
num	Virtual port number to which clients send requests (for example, 443).
ipaddr | **all**	Displays entries for the certificate associated with a specific server IP address or for all server IP addresses. The default is `all`.
sni	The full or partial SNI of the server from which the

Parameter	Description
	inside ACOS device imported the self-signed certificate and private key. • If you enter the IP address of the server, *sni* must be an exactly the same as in the certificate cache. You must enter the full SNI that is exactly the same as in the certificate cache. *sni*, The hashing activity for only that specific certificate is reported. • If you enter the keyword all, *sni* can be a partial match to the full server name. If a group of servers meets this partial match, all servers in this group are reported.

Usage The following field values appear in the output of this command :]

Field	Description
Real Server	This field specifies the gateway IP address and protocol port of the server that clients are trying to connect to.
Server Name	This field specifies the URL or SNI of the server that clients are trying to connect to.
state	• state: cert verifying The certificate of the server specified by the Real Server and Server Name fields is in the process of being verified. • state: cert forging The ACOS device is forging the certificate it will use for SSL sessions with clients trying to reach the specified server. • state: ready to forge The ACOS has verified the specified server's certificate is not revoked, and it is ready to forge certificates it will use for SSL sessions with clients trying to reach

Field	Description
	the specified server. • state: ready The forge certificate is in the ACOS cache.
hit times	The number of occurrences that a new session matches this certificate.
idle time	The amount of time since the previous hit.
timeout after	The certificate will be removed after this amount of idle time without any hits.
expires after	The certificate is removed after this amount of time has passed since the certificate was created.
serial (hex)	Certificate serial number in hexadecimal.

Default None

Mode All

Example The following example is for dynamic port SSLi:

```
ACOS# show slb ssl-forward-proxy-cert inside 0 ip 10.10.10.1
443 www.example.com
Virtual server (inside: 443):

----Start One Certificate---
real server: 74.6.143.25:443 tcp
server name: example.com
ALPN protocol: ALPN HTTP2
state: ready
hit times: 1
idle time: 3 seconds
timeout after 3597 seconds
expires after 604787 seconds
----End One Certificate---

1 hashed certificate retrieved
```

Example

The following example displays the certification information from Multi-PU platforms. The certificates of both PUs are merged.

```
ACOS(config)#show slb ssl-forward-proxy-cert vs_ep 3128 all

Virtual server (vs_ep: 3128):
----Start One Certificate---
real server: 200.0.60.96:443 tcp
server name: ax16-ssli-2.org
ALPN protocol: ALPN HTTP
state: ready
hit times: 1
idle time: 443 seconds
timeout after 3157 seconds
expires after 604347 seconds
----End One Certificate---

----Start One Certificate---
real server: 200.0.60.96:443 tcp
server name: ax16-ssli-11.org
ALPN protocol: ALPN HTTP
state: ready
hit times: 1
idle time: 1411 seconds
timeout after 2189 seconds
expires after 603379 seconds
version: 3
subject: SSL Certificate
common name: ssl-server.com
division: A10
locality: BJ
state or province: BJ
country name: CN
subject alternative name:
email:
start time: Nov 8 11:46:37 2018 GMT
expire time: Nov 5 11:46:41 2028 GMT
issuer: A10 Networks
serial(hex): 896f000000000534cc90
```

```
----End One Certificate---
```

show slb ssl-forward-proxy-stats

Description Show SSLi statistics.

For the Multi-PU platforms, the statistics display the aggregated counters; PU1 + PU2.

Syntax

```
show slb ssl-forward-proxy-stats
```

Default None

Mode All

Example The following example shows the counter fields.

```
ACOS(config)# show slb ssl-forward-proxy-stats
```

```
Bypass Failsafe SSL sessions:           2
Bypass Username sessions:               0
Bypass AD-Group sessions:               0
Bypass SNI sessions:                    0
Bypass Certificate subject sessions:    0
Bypass Certificate issuer sessions:     0
Bypass Certificate SAN sessions:        0
Bypass No SNI sessions:                 0
Bypass Client IP sessions:              0
Bypass Server IP sessions:              0
Reset No SNI sessions:                  0
Bypass ESNI sessions:                   0
Drop ESNI sessions:                     0
Bypass Client Auth sessions:            0
Failed in SSL handshakes:               0
Failed in crypto operations:            0
Failed in TCP:                          0
Failed in Certificate verification:     0
Failed in Certificate signing:          0
Invalid OCSP Stapling Response:         0
Revoked OCSP Response:                  0
Unsupported SSL version:                0
Bypass triggered by aFleX:              6
Certificates in cache:                  0
Certificates created:                   5
Certificates expired:                   5
Certificate cache hits:                 1578
Certificate cache miss:                 5
Connections bypassed:                   0
Connections inspected:                  1578
Connections failed:                     0
Total Async Connections:                0
Current Async Connections in Buffer:    0
Async Connections timeout:              0
Async Connections Queue full drop:      0
```

show slb ssl-ja3

Description Show the current numbers of JA3 amount.

For the Multi-PU platforms, the statistics displays the aggregated counters; PU1 + PU2.

Syntax

```
show slb ssl-ja3
```

Mode All

Example The following command shows the number of JA3:

```
ACOS#show slb ssl-ja3
Host           Numbers of JA3
-----------------------------
10.101.155.1   3
```

The following table describes the fields in the command output.

Field	Description
Host	Shows the host name or client IP address.
Number of JA3	Shows the current JA3 amount of client address.

show slb ssl-ja4

Description Show the current numbers of JA4 amount.

For the Multi-PU platforms, the statistics display the aggregated counters; PU1 + PU2.

Syntax

```
show slb ssl-ja4
```

Mode All

Example The following command shows the number of JA3:

```
ACOS#show slb ssl-ja4
Host           Numbers of JA4
-----------------------------
10.101.155.1   3
```

The following table describes the fields in the command output.

Field	Description
Host	Shows the host name or client IP address.
Number of JA4	Shows the current JA4 amount of client address.

show slb ssl-ocsp cache

Description Displays summarized contents of the SSL OCSP cache.

To handle large number of certificates, the pagination support is provided to retrieve the data in chunks. The amount of data requested is determined by the CLI display buffer capability which is 500 lines.

Syntax

```
show slb ssl-ocsp cache
```

Default None

Mode All

Usage The following table describes the fields in the command output:

Field	Description
Total	The total number of cached requests is listed.
Common Name	The common certificate name is listed.
Status	Good, revoked or unknown will appear to indicate certificate status.

Example The following example displays the contents of the SSL OSCP cache:

```
ACOS# show slb ssl-ocsp cache
Total: 2
Common Name
                          Status
-----------------------------------------------------------------
-----
Company1 Internet Authority
G2                                Good
```

```
Company2 Root Certificate Authority -
G2                      Good
```

Example The following example displays the summarized content of the PU2 SSL OSCP cache on the Multi-PU platforms:

```
ACOS#sh slb ssl-ocsp cache
Total: 841
Common Name                 Status  PU
-------------------------------------------
kohls.com                   Good    2
stamplive.com               Good    2
*.booking.com               Good    2
*.deezer.com                Good    2
urbandictionary.com         Good    2
```

show slb ssl-ocsp cache detail

Description Displays detailed contents of the SSL OCSP cache.

To handle large number of certificates, the pagination support is provided to retrieve the data in chunks. The amount of data requested is determined by the CLI display buffer capability which is 500 lines.

Syntax

```
show slb ssl-ocsp cache detail
```

Default None

Mode All

Usage The following table describes the fields in the command output:

Field	Description
Total	The total number of certificates in the ACOS cache
Name	Certificate name
Subject	Certificate subject name
Length:	Length of the certificate in bytes

Field	Description
URI:	URI of the certificate owner
Expire:	Time in seconds remaining before the certificate expires
Hits:	Number of times certificate was called from the cache by SSL proxy handshake with a client.
PU:	Processing Unit number in case of Multi-PU platform.

Example Use command to display information on SSL OCSP cache, including the name of the company, status, subject, length, URI, expiration, and number of hits.

```
ACOS# show slb ssl-ocsp cache detail
Total: 1
-----------------------------------------------------------------
-----
Name:    Company1 Internet Authority G2
Status:  Good
Subject: /C=US/O=Company1 Inc/CN=Company1 Internet Authority
G2
Length:  1012
URI:     http://a.example.com/
Expire:  17731488
Hits:    760
```

Example The following command displays the statistics of the Multi-PU platforms (from PU2).

The stored certificate content is displayed as a snapshot on each PU. Additionally, if the state (status) of the certificate changes while using this show command, the status will be reflected immediately.

```
ACOS(config)# show slb ssl-ocsp cache detail
Total: 841
-----------------------------------------------------------------
----------------
Name:    kohls.com
Status:  Good
Subject: /C=US/ST=Illinois/L=Aurora/O=Kohl's,
Inc./CN=kohls.com
Length:  2219
URI:     http://ocsp.digicert.com/
Expire:  575658
Hits:    0
PU:      2

Name:    stamplive.com
Status:  Good
Subject: /CN=stamplive.com
Length:  3501
URI:     http://r3.o.lencr.org/
Expire:  433094
Hits:    0
PU:      2

Name:    twitter.com
Status:  Good
Subject: /C=US/ST=California/L=San Francisco/O=Twitter, Inc.
Length:  1732
URI:     http://ocsp.digicert.com/
Expire:  586458
Hits:    0
PU:      2
```

```
Name:     *.momoshop.com.tw
Status:   Good
Subject: /C=TW/ST=Taiwan/L=Taipei/O=MOMO.COM
INC./CN=*.momoshop.com.tw
Length:   1843
URI:      http://twcasslocsp.twca.com.tw/
Expire:   272881
Hits:     0
PU:       2
```

show web-category

Description Shows the information about the current operation of the Web Category feature.

Syntax

```
show web-category
{bypassed-urls [num | all] |
database |
intercepted-urls [num | all] |
license |
statistics |
url-category name [local-db-only]
```

Syntax

```
show counters web-category
{category-list category-list-name | reputation-scope
reputation-scope-name}
```

Parameter	Description
bypassed-urls [*num* | **all**]	Lists the URLs bypassed by the Web Category feature. *num* – Specifies the number of URLs to list, 1-8000. The most recently bypassed URLs, up to the number you specify, are listed. **all** – Displays the entire list of URLs bypassed by the feature. The entries are listed beginning with the most recently bypassed URL on top. If a URL is

Parameter	Description
	bypassed multiple times, the URL is listed separately for each time it bypassed. By default, the 50 most recent entries are shown. **NOTE:** In case of Multi-PU platforms, if *num* is set to 100, 80 URLs from PU1 and 20 URLs from PU 2 will be displayed. Other bypassed URLs will not be displayed.
database	Shows information about the currently loaded BrightCloud database.
intercepted-urls [*num* | **all**]	Lists the URLs intercepted by the Web Category feature. *num* – Specifies the number of URLs to list, 1-8000. The most recently bypassed URLs, up to the number you specify, are listed. **all** – Displays the entire list of URLs bypassed by the feature. The entries are listed beginning with the most recently intercepted URL on top. If a URL is intercepted multiple times, the URL is listed separately for each time it intercepted. By default, the 50 most recent entries are shown. **NOTE:** In case of Multi-PU platforms, if *num* is set to 100, 80 URLs from PU1 and 20 URLs from PU 2 will be displayed. Other intercepted URLs will not be displayed.
license	Shows detailed information about the license.
url-category *url-name* **[local-db-only]**	Shows categories returned by BrightCloud library for the specified URL. **local-db-only** – Checks only the local database

Parameter	Description
	and service cache. Does not make a cloud query to fetch the category list for this URL.
category-list *category-list-name*	A list of web categories for web filtering or traffic categorization on the ACOS device.
reputation-scope	Configures the scope of the reputation score. The value can be greater-than or less-than the score level or customized score. And only one entry can be set in one scope for each greater-than or less-than setting.

Mode All

Example The following command shows the URLs bypassed by the Web Category feature:

```
ACOS#show web-category bypassed-urls
paper.example.com
paper.example.com
paper.example.com
paper.example.com
step.example.com
metrics1.example.com
step.example.com
paper.example.com
online.example.com
...
```

Example The following command shows information about the currently loaded BrightCloud database:

```
ACOS#show web-category database
Database Name                    : full_bcdb_rep_new_9.594.bin

Database Status                  : Active
Database Size                    : 351 MB
Database Version                 : 827
Last Update Time                 : Wed Jul  6 19:39:59 2016
Next Update Time                 : Fri Jul  8 00:00:22 2016
```

```
Connection Status                : GOOD
Last Successful Connection       : Thu Jul  7 00:39:22 2016
```

Example The following command shows the URLs intercepted by the Web Category feature:

```
ACOS#show web-category intercepted-urls
fhr.data.example.com
fhr.data.example.com
fhr.data.example.com
aus3.example.org
blocklist.addons.example.org
aus4.example.org
```

Default versioncheck-bg.addons.example.org

```
versioncheck-bg.addons.example.org
services.addons.example.org
aus3.example.org
fhr.data.example.com
...
```

Example The following commands show the web categories to which some individual URLs belong. In this example, the categories for the URLs in the ACOS Device's local database match the most recent categorizations from the BrightCloud server.

```
ACOS#show web-category url-category www.google.com
Search Engines
ACOS#show web-category url-category www.google.com local-db-
only
Search Engines
ACOS#show web-category url-category www.youtube.com
Streaming Media
ACOS#show web-category url-category www.youtube.com local-db-
only
Streaming Media
```

Example The following command displays the Web Category license information. Check the expiration date and status, and verify whether the configured SDK type is **Legacy** or **New**:

```
ACOS#show web-category license
Module Type                     : New
Module Status                   : Disabled
License Status                  : License is valid
License Type                    : show license-info for
webroot type
License Expiry                  : show license-info for
expiration
Remaining Period                : show license-info for
expiration
Grace Period Status             : show license-info for grace
period
Grace Period                    : show license-info for grace
period
UUID/SN                         : TH33075E2104003
```

Example The following command shows the hit count of web-category-list:

```
ACOS(config)#show counters web-category category-list test
show counters web-category category-list test
--------------------------------------
uncategorized category 0
real estate category 0
computer and internet security category 0
financial services category 0
...
...
...
self harm category 2
dns over https category 8
low-thc cannabis products category 10
artistic nudity 0
illegal pornography eg. child sexual abuse 0
```

Example The following command shows information on the web category from Multi-PU platforms:

- The blue highlighted text indicates the statistics from aggregated counters of PU1 and PU2.
- The bold text indicates the statistics from separate counters for PU1 and PU2.

```
ACOS(config)#show web-category statistics
```

```
Database lookups          : 2
Cloud cache lookups       : 3
Cloud lookups             : 2
RTU lookups               : 0
Lookup latency            : 194 msec
PU 1
                            Queue1    Queue2    Queue3    Queue4
   Queue5    Queue6    Queue7    Queue8    Queue9    Queue10
Queue11   Queue12   Queue13   Queue14   Queue15   Queue16
Queue17   Queue18   Queue19   Queue20   Queue21   Queue22
Queue23   Queue24   Queue25   Queue26   Queue27   Queue28
Queue29   Queue30   Queue31   Queue32   Queue33   Queue34
Queue35   Queue36   Queue37   Queue38   Queue39   Queue40
Queue41   Queue42   Total
-------------------------------------------------------------------
---------------------------
Requests in Queue          0          0          0          0
   0          0          0          0          0          0
0          0          0          0          0          0          0
       0          0          0          0          0          0
    0          0          0          0          0          0
 0          0          0          0          0          0          0
        0          0          0          0          0          0
     0

Requests dropped           0          0          0          0
   0          0          0          0          0          0
0          0          0          0          0          0          0
       0          0          0          0          0          0
    0          0          0          0          0          0
 0          0          0          0          0          0          0
        0          0          0          0          0          0
     0
Requests processed         0          0          0          0
   0          0          0          0          0          0
0          0          0          0          0          0          0
       0          0          0          0          0          0
    0          1          0          0          0          0
```

```
 0          0          0          0          0          0          0
        0          0          0          0          0          0
     1

PU 2
                           Queue1     Queue2     Queue3     Queue4
   Queue5     Queue6     Queue7     Queue8     Queue9     Queue10
Queue11    Queue12    Queue13    Queue14    Queue15    Queue16
Queue17    Queue18    Queue19    Queue20    Queue21    Queue22
Queue23    Queue24    Queue25    Queue26    Queue27    Queue28
Queue29    Queue30    Queue31    Queue32    Queue33    Queue34
Queue35    Queue36    Queue37    Queue38    Queue39    Queue40
Queue41    Queue42    Total
-------------------------------------------------------------------
---------------------------
Requests in Queue          0          0          0          0
   0          0          0          0          0          0
0          0          0          0          0          0          0
       0          0          0          0          0          0
    0          0          0          0          0          0
 0          0          0          0          0          0          0
        0          0          0          0          0          0
     0

Requests dropped           0          0          0          0
   0          0          0          0          0          0
0          0          0          0          0          0          0
       0          0          0          0          0          0
    0          0          0          0          0          0
 0          0          0          0          0          0          0
        0          0          0          0          0          0
     0

Requests processed         0          0          0          0
   0          0          0          0          0          0
0          0          0          0          0          0          0
       0          0          0          0          0          0
    0          0          0          1          0          0
```

```
 0          0          0          0          0          0          0
        0          0          0          0          0          0
     1
PU 1
                           Lookup1    Lookup2    Lookup3
Lookup4    Lookup5    Total
------------------------------------------------------------------
--------------------
Requests processed         0          1          0          0
   0          1
PU 2
                           Lookup1    Lookup2    Lookup3
Lookup4    Lookup5    Total
------------------------------------------------------------------
--------------------
Requests processed         0          0          0          0
   1          1

Memory Stats:
Database Memory          : 1147 MB
RTU Cache Memory         : 0 bytes
Lookup Cache Memory      : 161 MB
```

Example The following command displays the counters specific to a category list within the configured web-category.

```
vThunder(config)#show counters web-category category-list
list1

show counters web-category category-list list1
--------------------------------------
uncategorized category
  0
real estate category
  0
computer and internet security category
  0
financial services category
  0
business and economy category
  0
computer and internet info category
  2
```

show web-reputation

Description Displays the URLs which are bypassed/intercepted by web-reputation rules in client-ssl template and checks the reputation score for the specific URLs.

Syntax

```
show web-reputation {bypassed-urls | intercepted-urls | url-reputation URL name}
```

Option	Description
bypassed-urls	Show the list of bypassed URLs, when the request is bypassed by web reputation rules.
intercepted-urls	Show the list of intercepted URLs, when the request is intrecepted by web reputation rules.
url-reputation	Show the URL reputation score returned by BrightCloud library for a URL.

Mode SLB client SSL template show mode

Example The following command shows the URLs bypassed by the web reputation feature:

```
ACOS#show web-reputation bypassed-urls
Score     URL
79        www.77file.com
81        www.testing.com
81        a10networks.com
...
```

Example The following command shows the URLs intercepted by the web reputation feature:

```
ACOS#show web-reputation intercepted-urls
Score     URL
10        17ebook.com
40        gerry90160.a10-tplab.com
54        earn4files.com
```

Example The following commands show the web reputation scores of the URLs:

```
ACOS#show web-reputation url-reputation www.google.com local-
db-only
trustworthy(81)
ACOS# show show web-reputation url-reputation www.google.com
trustworthy(81)
ACOS# show web-reputation url-reputation www.abc.com local-db-
only
can not find reputation score from local database
ACOS# show web-reputation url-reputation www.abc.com
trustworthy(96)
```

Cloud Services

This reference lists the CLI configuration and show commands that apply specifically to the cloud services for centralized monitoring.

Configuration Commands

cloud-services

Description Specifies configuration for different cloud providers.

Syntax

```
[no] cloud-services
{
cloud-provider { aws | azure | vmware }|
meta-data
}
```

Parameter	Description
cloud-provider	Configures the cloud-provider.
meta-data	Configures the user-data services. **NOTE:** This option works only with the shared active-partition.

This command changes the CLI to the configuration level for the specified **cloud-provider**, where the following additional commands are available:

Parameter	Description
aws	Publishes the enabled metric/s, logs, or both to AWS CloudWatch. For more information, see cloud-services cloud-

Parameter	Description
	provider aws command.
azure	Publishes the enabled metric/s to Azure Application Insights and logs to Azure Log Analytics Workspace. For more information, see cloud-services cloud-provider azure command.
vmware	Publishes the enabled metric/s to VMware vRealize Operations (vROps) and logs to vRealize Log Insight (vRLI). For more information, see cloud-services cloud-provider vmware command.

Default None

Mode Configuration Mode

Usage This command publishes the vThunder-ADC logs, metrics, or both to the configured cloud monitoring service.

Example The following commands enable AWS as the cloud provider for publishing vThunder log, metrics, or both:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
```

cloud-services cloud-provider

Description Specifies the configuration to publish the vThunder ADC log, metrics, or both to a specific cloud provider.

Syntax

```
[no] cloud-services cloud-provider { aws | azure | vmware }
```

Parameter	Description
aws	Publishes the selected metric/s, logs, or both to AWS CloudWatch.

Parameter	Description
azure	Publishes the selected metric/s to Azure Application Insights and logs to Azure Log Analytics Workspace.
vmware	Publishes the selected metric/s to VMware vRealize Operations (vROps) and logs to vRealize Log Insight (vRLI).

Default None

Mode Privileged Mode

Example The following commands enable AWS as the cloud provider for publishing vThunder log, metrics, or both:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
```

Related Commands:

- admin cloud-cred

cloud-services cloud-provider aws

Description Configures AWS as the cloud-provider for exporting the vThunder ADC logs, metrics, or both, and for setting up vThunder instances in High Availability (HA) mode across different availability zones.

Syntax

```
[no] cloud-services cloud-provider aws
{
log options |
metrics options |
multi-az-failover options
}
```

Parameter	Description
log *options*	Enables, disables, or configures vThunder ADC log monitoring for AWS. For AWS log *options*, see cloud-services cloud-

Parameter	Description
	provider aws log command.
metrics *options*	Enables, disables, or configures vThunder ADC metrics monitoring for AWS. For AWS metrics *options*, see cloud-services cloud-provider aws metrics command.
multi-az-failover *options*	Configures vThunder in High Availability (HA) mode across different availability zones. For AWS multi-az-failover *options*, see cloud-services cloud-provider aws multi-az-failover command.

Default None

Mode Privileged EXEC

Usage This command enables performance metrics monitoring and publishes the enabled vThunder metrics on the AWS platform where the vThunder instance is deployed. It enables syslog monitoring and publishes vThunder Syslogs on the AWS platform where the vThunder instance is deployed or to any Azure or VMware platforms. It also allows the configuration of vThunder instances in High Availability (HA) fail-over mode across different availability zones (AZ) within the same VPC of an AWS region. With the **multi-az-failover** option enabled, the standby vThunder instance can take over if the active instance fails, even if they are in different AZs.

Example The following commands enable log monitoring for AWS:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#log
ACOS(config-cloud-provider-aws-log)#enable
```

Example The following commands enable metrics monitoring for AWS:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#metrics
ACOS(config-cloud-provider-aws-metrics)#enable
```

Example The following commands enable High Availability (HA) fail-over mode across different availability zones (AZ):

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#multi-az-failover
```

cloud-services cloud-provider aws log

Description Configures the vThunder ADC syslog monitoring on AWS CloudWatch.

Syntax

```
[no] cloud-services cloud-provider aws log
{
enable |
disable |
log-group-name name |
active-partitions name
}
```

Parameter	Description
enable	Enables the vThunder ADC log monitoring for AWS.
disable	Disables the vThunder ADC log monitoring for AWS. By default, it is disabled.
log-group-name *name*	Specifies the name of the log group under which all the logs are sent to the AWS CloudWatch.
active-partitions *name*	Specifies one or more comma-separated partitions for which the vThunder logs are viewed. By default, the active partition is "Shared". **For example**: "SHARED, Px"

Parameter	Description
	The maximum number of partitions supported per vThunder is 20. Only L3V active partitions are supported. To view the vThunder logs of all active partitions, specify "*". **NOTE:** The last updated active partitions configured through CLI or aXAPI is used to publish metrics and logs on AWS.

Default None

Mode Privileged EXEC

Usage The vThunder ADC syslogs are displayed on AWS CloudWatch only when the log monitoring is enabled for AWS.

Example The following commands enable the vThunder syslogs for P1 and P2 partitions on AWS CloudWatch:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#log
ACOS(config-cloud-provider-aws-log)#enable
ACOS(config-cloud-provider-aws-log)#log-group-name vThunder
ACOS(config-cloud-provider-aws-log)#active-partitions P1, P2
```

cloud-services cloud-provider aws metrics

Description Configures the vThunder ADC metrics monitoring on AWS CloudWatch.

Syntax

```
[no] cloud-services cloud-provider aws metrics
{
cps { enable | disable } |
cpu { enable | disable } |
disk { enable | disable } |
enable |
disable |
interfaces { enable | disable } |
memory { enable | disable } |
namespace name |
```

```
packet-drop { enable | disable } |
packet-rate { enable | disable } |
server-down-count { enable | disable } |
server-down-percentage { enable | disable } |
server-error { enable | disable } |
sessions { enable | disable } |
ssl-cert { enable | disable } |
throughput { enable | disable } |
tps { enable | disable } |
active-partitions name
}
```

Parameter	Description
cps {enable | disable}	Enables or disables the metrics for displaying the count of the new connections per second.
cpu {enable | disable}	Enables or disables the metrics for displaying the average data CPU usage, in percentage.
disk { enable | disable }	Enables or disables the metrics for displaying the average disk storage usage, in percentage.
enable	Enables the vThunder ADC metrics monitoring for AWS.
disable	Disables the vThunder ADC metrics monitoring for AWS. By default, it is disabled.
interfaces { enable | disable }	Enables or disables the metrics for displaying the count of the total data network interfaces.
memory { enable | disable }	Enables or disables the metrics for displaying the memory (RAM) usage, in

Parameter	Description
	percentage.
namespace *name*	Specifies the AWS namespace where all the metrics must be published.
packet-drop { enable | disable }	Enables or disables the metrics for displaying the count of the total packets dropped while sending data from or receiving data at the vThunder instance.
packet-rate { enable | disable }	Enables or disables the metrics for displaying the count of the total packets sent from or received at the vThunder instance.
server-down-count { enable | disable }	Enables or disables the metrics for displaying the Count of the total web or app servers configured in the vThunder instance that are not reachable from vThunder.
server-down-percentage { enable | disable }	Enables or disables the metrics for displaying the percentage of the total web or app servers configured in the vThunder instance that are not reachable from vThunder.

Parameter	Description
server-error { enable | disable }	Enables or disables the metrics for displaying the count of the total errors that occurred during data transmission from vThunder to the server with status codes 4xx and 5xx.
sessions { enable | disable }	Enables or disables the metrics for displaying the count of the total active sessions of the vThunder instance.
ssl-cert { enable | disable }	Enables or disables the metrics for displaying the count of the total errors that occurred during data transmission from vThunder to the server due to SSL connection, negotiate, encrypt, and decrypt.
throughput { enable | disable }	Enables or disables the metrics for displaying the total vThunder system global throughput bits per sec from vThunder instance to the server.
tps { enable | disable }	Enables or disables the metrics for displaying the count of the total L7 transactions made per second from vThunder instance to the server.

Parameter	Description
active-partitions *name*	Specifies one or more comma-separated partition/s for which the vThunder metrics is viewed. By default, the active partition is "Shared". **For example**: "SHARED, Px" The maximum number of partitions supported per vThunder is 20. Only L3V active partitions are supported. To view the vThunder metrics of all active partitions, specify "*". **NOTE:** The last updated active partitions configured through CLI or aXAPI is used to publish metrics and logs on AWS.

Default All metrics are disabled.

Mode Privileged EXEC

Usage The selected vThunder ADC metrics are displayed on AWS CloudWatch only when the metrics monitoring is enabled for AWS.

Example The following commands enable the vThunder CPU and memory usage metrics for P1 and P2 partitions on AWS CloudWatch:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#metrics
ACOS(config-cloud-provider-aws-metrics)#enable
ACOS(config-cloud-provider-aws-metrics)#active-partitions P1,
P2
ACOS(config-cloud-provider-aws-metrics)#namespace vThunder
ACOS(config-cloud-provider-aws-metrics)#cpu enable
ACOS(config-cloud-provider-aws-metrics)#memory enable
```

Example The following commands enable the vThunder CPS metrics for all partitions on AWS CloudWatch:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#metrics
ACOS(config-cloud-provider-aws-metrics)#enable
ACOS(config-cloud-provider-aws-metrics)#active-partitions *
ACOS(config-cloud-provider-aws-metrics)#namespace vThunder
ACOS(config-cloud-provider-aws-metrics)#cps enable
```

cloud-services cloud-provider aws multi-az-failover

Description Configures the vThunder instances to support HA fail-over across different Availability Zones (AZ) within the same VPC of an AWS region.

Syntax

```
[no] cloud-services cloud-provider aws multi-az-failover
{
 vrid num
 {
 fip-dest name |
 fip-interface-id name |
 route-table-id name |
 user-tag |
 vip num { elastic-ip IP_address | private-ip IP_address } |
 vip-dest name |
 vip-interface-id name
 }
}
```

Parameter	Description
vrid *num*	

Parameter	Description
	Specifies the VRRP-A virtual router ID (VRID) number <0-31> to be used in the high availability configuration. This command changes the CLI to the configuration level for the specified VRID.
fip-dest *name*	Specifies the destination CIDR block (1-64 characters) for an alien floating IP (FIP). An alien FIP is an external IP address used to route traffic. It is used to define the IP address range that the floating IP can either target or be routed to.
fip-interface-id *name*	Specifies the interface ID (1-64 alphanumeric characters) for outgoing data (data-out) associated with the floating IP. It is used to identify the network interface on the vThunder instance for the floating IP's outbound traffic.
route-table-id *name*	Specifies the ID of the AWS route table ID associated with the network interface. It is used for routing traffic.
vip *num* { **elastic-ip** *IPv4_address* | **private-ip** *IPv4_address* }	Specifies a list of Virtual IP (VIP) addresses (0-2147483647) and the type of the associated IP address. It is used to define the VIPs that will be managed by the vThunder instance. The following IP addresses are supported: • **elastic-ip** *IPv4_address* - Specifies a public IPv4 address provided by AWS. When an elastic IP is associated with the VIP, a consistent public IP address is maintained, even if the underlying instance changes during failover.

Parameter	Description
	• **private-ip** *IPv4_address* - Specifies an Alien IPv4 address that is used within a VPC but is not originally part of the AWS VPC IP range. When a private IP is associated with the VIP, only internal network traffic reaches the server.
vip-dest *name*	Specifies the destination CIDR block (1-64 alphanumeric characters) for an alien virtual IP. An alien VIP is an external VIP address. It is used to define the IP address range that the virtual IP can either target or be routed to.
vip-interface-id *name*	Specifies the interface ID (1-64 characters) for incoming data (data-in) associated with the VIP. It is used to identify the network interface on the vThunder instance for the virtual IP's inbound traffic.

Default Disabled

Mode Privileged EXEC

Usage When vThunder instances are configured for High Availability (HA) across different AZs within the same VPC of an AWS region, the vThunder instances work together as an HA cluster across AZs. If one vThunder instance becomes unavailable during fail-over, another can take over and continue to serve requests.

Example The following commands configure HA-failover for vThunder instances across different Availability Zone (AZ) using Elastic IP address:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#multi-az-failover
ACOS(config-cloud-provider-aws-multi-az-f...)#vrid num
ACOS(config-cloud-provider-aws-multi-az-f...)#vip-interface-id
name
ACOS(config-cloud-provider-aws-multi-az-f...)#vip num
ACOS(config-cloud-provider-aws-multi-az-f...)#private-ip IP_
address
ACOS(config-cloud-provider-aws-multi-az-f...)#elastic-ip IP_
address
```

Example The following commands configure HA-failover for vThunder instances across different Availability Zone (AZ) using Private (Alien) IP:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#multi-az-failover
ACOS(config-cloud-provider-aws-multi-az-f...)#vrid num
ACOS(config-cloud-provider-aws-multi-az-f...)#route-table-id
name
ACOS(config-cloud-provider-aws-multi-az-f...)#vip-interface-id
name
ACOS(config-cloud-provider-aws-multi-az-f...)#fip-interface-id
name
ACOS(config-cloud-provider-aws-multi-az-f...)#vip-dest name
ACOS(config-cloud-provider-aws-multi-az-f...)#fip-dest name
```

cloud-services cloud-provider azure

Description Configures Azure as the cloud-provider for exporting the vThunder ADC logs, metrics, or both.

Syntax

```
[no] cloud-services cloud-provider azure
{
log options |
metrics options
}
```

Parameter	Description
log *options*	Enables, disables, or configures vThunder ADC log monitoring for Azure. For Azure log *options*, see cloud-services cloud-provider azure log.
metrics *options*	Enables, disables, or configures vThunder ADC metrics monitoring for Azure. For Azure metrics *options*, see cloud-services cloud-provider azure metrics.

Default None

Mode Privileged EXEC

Usage This command enables performance metrics monitoring and publishes the enabled vThunder metrics on the Azure platform where the vThunder instance is deployed. It also enables syslog monitoring and publishes vThunder Syslogs on the Azure platform where the vThunder instance is deployed or to any AWS or VMware platforms.

Example The following commands enable log monitoring for Azure:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#log
ACOS(config-cloud-provider-azure-log)#enable
```

Example The following commands enable metrics monitoring for AWS:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#metrics
ACOS(config-cloud-provider-azure-metrics)#enable
```

cloud-services cloud-provider azure log

Description Configures the vThunder ADC syslog monitoring on Azure Log Analytics Workspace.

Syntax

```
[no] cloud-services cloud-provider azure log
{
enable |
disable |
resource-id num |
workspace-id num |
active-partitions name
}
```

Parameter	Description
enable	Enables the vThunder ADC log monitoring for Azure.
disable	Disables the vThunder ADC log monitoring for Azure.
resource-id *num*	Specifies the compute instance resource ID or the instance ID on which vThunder is deployed. To get this value, go to **Azure Portal** > **Azure services** > **Virtual machine** > <*your_vThunder_instance*> > **Setting** > **Properties** and get the **Resource ID** from the right panel.
workspace-id *num*	Specifies the Azure Log Analytics Workspace ID. To get this value, go to **Azure Portal** > **Azure services** > **Log Analytics workspaces** > <*your_log_analytics_workspace*> > **Settings** > **Agents**.
active-partitions *name*	Specifies one or more comma-separated partition/s for which the vThunder logs are viewed. By default, the active partition is "Shared". **For example**: "SHARED, Px" The maximum number of partitions supported per vThunder is 20. Only L3V active partitions are supported. To view the vThunder logs of all active partitions, specify "*".

Parameter	Description
	NOTE: The last updated active partitions configured through CLI or aXAPI is used to publish metrics and logs on Azure.

Default None

Mode Privileged EXEC

Usage The vThunder syslogs are displayed on Azure Log Analytics Workspace only when the log monitoring is enabled for Azure.

Example The following commands enable the vThunder syslogs for P1 and P2 partitions on Azure Log Analytics Workspace:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#log
ACOS(config-cloud-provider-azure-log)#enable
ACOS(config-cloud-provider-azure-log)#resource-id
/subscriptions/07d34b9b-61e3-475a-abbc-
006b16812a3e/resourceGroups/vth-
rg6/providers/microsoft.insights/components/vth-vmss-app-
insights
ACOS(config-cloud-provider-azure-log)#workspace-id dcfd78d5-
3a49-425d-8410-e02e281f7991
ACOS(config-cloud-provider-azure-log)#active-partitions P1, P2
```

cloud-services cloud-provider azure metrics

Description Configures the vThunder ADC and TPS metrics monitoring on Azure monitoring tools.

Syntax

```
[no] cloud-services cloud-provider azure metrics
{
cps { enable | disable } |
cpu { enable | disable } |
disk { enable | disable } |
ddos |
enable |
disable |
interfaces { enable | disable } |
```

```
memory { enable | disable } |
resource-id num |
packet-drop { enable | disable } |
packet-rate { enable | disable } |
server-down-count { enable | disable } |
server-down-percentage { enable | disable } |
server-error { enable | disable } |
sessions { enable | disable } |
ssl-cert { enable | disable } |
throughput { enable | disable } |
tps { enable | disable } |
active-partitions name
}
```

Parameter	Description
cps { enable | disable }	Enables or disables the metrics for displaying the count of the new connections per second.
cpu { enable | disable }	Enables or disables the metrics for displaying the average data CPU usage, in percentage.
disk { enable | disable }	Enables or disables the metrics for displaying the average disk storage usage, in percentage.
ddos	Configures the vThunder DDoS performance metrics monitoring on Azure Monitor. This command changes the configuration mode to a sub-mode where the following commands are available:

Parameter	Description
	• **entry-zone** { enable | disable } - Enables or disables all the DDoS entries and zones statistics. • **port** { enable | disable } - Enables or disables all the port statistics. • **tcp** { enable | disable } - Enables or disables all the TCP protocol statistics. • **udp** { enable | disable } - Enables or disables all the UDP protocol statistics.
enable	Enables the vThunder ADC metrics monitoring for Azure.
disable	Disables the vThunder ADC metrics monitoring for Azure. By default, it is disabled.
interfaces { enable | disable }	Enables or disables the metrics for displaying the count of the total data network interfaces.

Parameter	Description
memory { enable | disable }	Enables or disables the metrics for displaying the memory (RAM) usage, in percentage.
resource-id *num*	Specifies the Azure Application Insights resource ID or the Instance Resource ID. To get this value, go to **Azure Portal** > **Azure services** > **Virtual machine** > <*your_vThunder_instance*> > **Setting** > **Properties** and get the **Resource ID** from the right panel.
packet-drop { enable | disable }	Enables or disables the metrics for displaying the count of the total packets dropped while sending data from or receiving data at the vThunder instance.
packet-rate { enable | disable }	Enables or disables the metrics for displaying the count of the total packets sent from or received at the vThunder instance.
server-down-count { enable | disable }	Enables or disables the metrics for displaying the Count of the total web or app servers

Parameter	Description
	configured in the vThunder instance that are not reachable from vThunder.
server-down-percentage { enable | disable }	Enables or disables the metrics for displaying the percentage of the total web or app servers configured in the vThunder instance that are not reachable from vThunder.
server-error { enable | disable }	Enables or disables the metrics for displaying the count of the total errors that occurred during data transmission from vThunder to the server with status codes 4xx and 5xx.
sessions { enable | disable }	Enables or disables the metrics for displaying the count of the total active sessions of the vThunder instance.
ssl-cert { enable | disable }	Enables or disables the metrics for displaying the count of the total errors that occurred during data transmission from vThunder to the server due to SSL connection,

Parameter	Description
	negotiate, encrypt, and decrypt.
throughput { enable | disable }	Enables or disables the metrics for displaying the total vThunder system global throughput bits per sec from vThunder instance to the server.
tps { enable | disable }	Enables or disables the metrics for displaying the count of the total L7 transactions made per second from vThunder instance to the server.
active-partitions *name*	Specifies one or more comma-separated partition/s for which the vThunder metrics is viewed. By default, the active partition is "Shared". **For example**: "SHARED, Px" The maximum number of partitions supported per vThunder is 20. Only L3V active partitions are supported. To view the vThunder

Parameter	Description
	metrics of all active partitions, specify "*". **NOTE:** The last updated active partitions configured through CLI or aXAPI is used to publish metrics and logs on Azure.

Default All metrics are disabled.

Mode Privileged EXEC

Usage When the metrics monitoring is configured, the selected vThunder metrics are displayed for ADC on Azure Application Insights.
When the metrics monitoring is configured specifically for **ddos**, the selected vThunder metrics for TPS sub-options are displayed on Azure Monitor.

Example The following commands enable the vThunder CPU and memory usage metrics for P1 and P2 partitions on Azure Application Insights:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#metrics
ACOS(config-cloud-provider-azure-metrics)#enable
ACOS(config-cloud-provider-azure-metrics)#active-partitions
P1, P2
ACOS(config-cloud-provider-azure-metrics)#resource-id
/subscriptions/07d34b9b-61e3-475a-abbc-
006b16812a3e/resourceGroups/vth-
rg6/providers/microsoft.insights/components/vth-vmss-app-
insights
ACOS(config-cloud-provider-azure-metrics)#cpu enable
ACOS(config-cloud-provider-azure-metrics)#memory enable
```

Example The following commands enable the vThunder CPS metrics for all partitions on Azure Application Insights:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#metrics
ACOS(config-cloud-provider-azure-metrics)#enable
ACOS(config-cloud-provider-azure-metrics)#active-partitions *
ACOS(config-cloud-provider-azure-metrics)#resource-id
/subscriptions/07d34b9b-61e3-475a-abbc-
006b16812a3e/resourceGroups/vth-
rg6/providers/microsoft.insights/components/vth-vmss-app-
insights
ACOS(config-cloud-provider-azure-metrics)#cps enable
```

Example The following configuration enables DDoS metric monitoring on Azure:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#azure
ACOS(config-cloud-provider-azure)#metrics
ACOS(config-cloud-provider-azure-metrics)#enable
ACOS(config-cloud-provider-azure-metrics)#ddos
ACOS(config-cloud-provider-azure-metrics-...)#entry-zone
enable
ACOS(config-cloud-provider-azure-metrics-...)#port enable
ACOS(config-cloud-provider-azure-metrics-...)#tcp enable
ACOS(config-cloud-provider-azure-metrics-...)#udp enable
```

cloud-services cloud-provider vmware

Description Configures VMware as the cloud-provider for exporting the vThunder ADC logs, metrics, or both.

Syntax

```
[no] cloud-services cloud-provider vmware
{
log options |
metrics options
}
```

Parameter	Description
log *options*	Enables, disables, or configures vThunder ADC log monitoring for VMware. For VMware log *options*, see cloud-services cloud-provider vmware log.
metrics *options*	Enables, disables, or configures vThunder ADC log monitoring for VMware. For VMware metrics *options*, see cloud-services cloud-provider vmware metrics.

Default None

Mode Privileged EXEC

Usage This command enables performance metrics monitoring and publishes the enabled vThunder metrics on the VMware platform where the vThunder instance is deployed. It also enables syslog monitoring and publishes vThunder Syslogs on the VMware platform where the vThunder instance is deployed or to any AWS or Azure platforms.

Example The following commands enable log monitoring for VMware:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware)#log
ACOS(config-cloud-provider-vmware-log)#enable
```

Example The following commands enable metrics monitoring for VMware:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware)#metrics
ACOS(config-cloud-provider-vmware-metrics)#enable
```

cloud-services cloud-provider vmware log

Description Configures the vThunder ADC syslog monitoring on VMware vRealize Log Insight (vRLI).

Syntax

```
[no] cloud-services cloud-provider vmware log
{
enable |
disable |
vrli-host name |
active-partitions name
}
```

Parameter	Description
enable	Enables the vThunder ADC log monitoring for VMware.
disable	Disables the vThunder ADC log monitoring for VMware. By default, it is disabled.
vrli-host *name*	Specifies the VMware vRLI host IP address.
active-partitions *name*	Specifies one or more comma-separated partition/s for which the vThunder logs are viewed. By default, the active partition is "Shared". **For example**: "SHARED, Px" The maximum number of partitions supported per vThunder is 20. Only L3V active partitions are supported. To view the vThunder logs of all active partitions, specify "*". **NOTE:** The last updated active partitions configured through CLI or aXAPI is used to publish metrics and logs on VMware.

Default None

Mode Privileged EXEC

Usage The vThunder ADC syslogs are displayed on VMware vRLI only when the vThunder ADC log monitoring is enabled for VMware.

Example The following commands enable the vThunder syslogs for P1 and P2 partitions on VMware vRealize Log Insight:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware)#log
ACOS(config-cloud-provider-vmware-log)#enable
ACOS(config-cloud-provider-vmware-log)#vrli-host 10.67.4.13
ACOS(config-cloud-provider-vmware-log)#active-partitions P1,
P2
```

cloud-services cloud-provider vmware metrics

Description Configures the vThunder ADC metrics monitoring on VMware vRealize Operations Manager (vROps).

Syntax

```
[no] cloud-services cloud-provider vmware metrics
{
cps { enable | disable } |
cpu { enable | disable } |
disk { enable | disable } |
enable |
disable |
interfaces { enable | disable } |
memory { enable | disable } |
resource-id num |
packet-drop { enable | disable } |
packet-rate { enable | disable } |
server-down-count { enable | disable } |
server-down-percentage { enable | disable } |
server-error { enable | disable } |
sessions { enable | disable } |
ssl-cert { enable | disable } |
throughput { enable | disable } |
tps { enable | disable } |
vrops-host num
active-partitions name
}
```

Parameter	Description
cps { enable | disable }	Enables or disables the metrics for displaying the count of the new connections per second.

Parameter	Description
cpu { enable | disable }	Enables or disables the metrics for displaying the average data CPU usage, in percentage.
disk { enable | disable }	Enables or disables the metrics for displaying the average disk storage usage, in percentage.
enable	Enables the vThunder ADC metrics monitoring for VMware.
disable	Disables the vThunder ADC metrics monitoring for VMware By default, it is disabled.
interfaces { enable | disable }	Enables or disables the metrics for displaying the count of the total data network interfaces.
memory { enable | disable }	Enables or disables the metrics for displaying the memory (RAM) usage, in percentage.
resource-id *num*	Specifies the compute instance resource ID on which vThunder is deployed. To get this value, go to **vRealize Operations**

Parameter	Description
	Web UI Home > **Environment** > **Object Browser** > **All Objects** > **vCenter Adapter** > **Virtual Machine** > **vThunder** and get the resource ID from the URL.
packet-drop { enable | disable }	Enables or disables the metrics for displaying the count of the total packets dropped while sending data from or receiving data at the vThunder instance.
packet-rate { enable | disable }	Enables or disables the metrics for displaying the count of the total packets sent from or received at the vThunder instance.
server-down-count { enable | disable }	Enables or disables the metrics for displaying the Count of the total web or app servers configured in the vThunder instance that are not reachable from vThunder.
server-down-percentage { enable | disable }	Enables or disables the metrics for displaying the percentage of the total web or app servers configured in

Parameter	Description
	the vThunder instance that are not reachable from vThunder.
server-error { enable | disable }	Enables or disables the metrics for displaying the count of the total errors that occurred during data transmission from vThunder to the server with status codes 4xx and 5xx.
sessions { enable | disable }	Enables or disables the metrics for displaying the count of the total active sessions of the vThunder instance.
ssl-cert { enable | disable }	Enables or disables the metrics for displaying the count of the total errors that occurred during data transmission from vThunder to the server due to SSL connection, negotiate, encrypt, and decrypt.
throughput { enable | disable }	Enables or disables the metrics for displaying the total vThunder system global throughput bits per sec from vThunder instance to the server.

Parameter	Description
tps { enable | disable }	Enables or disables the metrics for displaying the count of the total L7 transactions made per second from vThunder instance to the server.
vrops-host *num*	Specifies the VMware vROps host IP address.
active-partitions *name*	Specifies one or more comma-separated partition/s for which the vThunder metrics is viewed. By default, the active partition is "Shared". **For example**: "SHARED, Px" The maximum number of partitions supported per vThunder is 20. Only L3V active partitions are supported. To view vThunder metrics of all active partitions, specify "*".

Parameter	Description
	NOTE: The last updated active partitions configured through CLI or aXAPI is used to publish metrics and logs on VMware.

Default All metrics are disabled.

Mode Privileged EXEC

Usage The selected vThunder ADC metrics are displayed on VMware vROps only when the metrics monitoring is enabled for VMware.

Example The following commands enable the vThunder CPU and memory usage metrics for P1 and P2 partitions on VMware vROps:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware)#metrics
ACOS(config-cloud-provider-vmware-metrics)#enable
ACOS(config-cloud-provider-vmware-metrics)#active-partitions
P1, P2
ACOS(config-cloud-provider-vmware-metrics)#vrops-host
10.67.4.13
ACOS(config-cloud-provider-vmware-metrics)#resource-id
3ae28ba2-c8b9-497f-8b98-76bedc93f31c
ACOS(config-cloud-provider-vmware-metrics)#cpu enable
ACOS(config-cloud-provider-vmware-metrics)#memory enable
```

Example The following commands enable the vThunder CPS metrics for all partitions on VMware vROps:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#vmware
ACOS(config-cloud-provider-vmware)#metrics
ACOS(config-cloud-provider-vmware-metrics)#enable
ACOS(config-cloud-provider-vmware-metrics)#active-partitions *
ACOS(config-cloud-provider-vmware-metrics)#vrops-host
10.67.4.13
ACOS(config-cloud-provider-vmware-metrics)#resource-id
3ae28ba2-c8b9-497f-8b98-76bedc93f31c
ACOS(config-cloud-provider-vmware-metrics)#cps enable
```

Contact Us

©2025 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.