



ACOS 6.0.7

Command Line Interface Reference

June, 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 Baselineing 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	103
Configuration Commands	103
Privileged EXEC	103
axdebug	103
backup log	118
backup system	120

clear	122
clock	123
configure	124
diff	124
disable	125
exit	126
export	126
gen-server-persist-cookie	130
health-test	131
help	132
import	132
locale	149
no	150
ping	151
reboot	153
reload	156
repeat	157
shutdown	157
ssh	158
telnet	159
terminal	160
traceroute	162
write force	163
write memory	164
write terminal	166
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	207
admin-session clear	208
aflex	209
aflex-scripts start	209
arp	210
arp-timeout	210
audit	211
authentication console type	212
authentication enable	213
authentication login privilege-mode	213
authentication mode	214
authentication multiple-auth-reject	215
authentication type	216
authorization	217
automatic-update	219
backup store	229

backup-periodic	230
banner	233
bfd echo	234
bfd enable	234
bfd interval	234
block-abort	235
block-merge-end	236
block-merge-start	236
block-replace-end	237
block-replace-start	237
boot-block-fix	238
bootimage	238
bpdu-fwd-group	239
bridge-vlan-group	240
chassis-application-type	242
class-list	243
class-list (for Aho-Corasick)	244
class-list (for IP limiting)	245
class-list (for VIP-based DNS caching)	248
class-list (for many pools, non-LSN)	250
class-list (string)	252
class-list (string-case-insensitive)	252
configure sync	253
copy	255
delete	257
disable reset statistics	259
disable slb	260
disable-failsafe	260
disable-management	261
dnssec	264
do	267

domain-list	268
enable reset statistics	269
enable-core	270
enable-management	270
enable-password	274
end	274
environment temperature threshold	275
environment update-interval	276
erase	278
event	280
exit	280
fail-safe	281
fan-speed	283
file-system	284
glid	285
glm	290
hd-monitor enable	290
health global	291
health monitor	293
health source-nat	294
health-test	296
hostname	296
hsm template	297
hsm template template-name softHSM	297
hsm template template-name thalesHSM	297
icmp-rate-limit	299
icmpv6-rate-limit	300
import	301
import-periodic	319
import-periodic geo-location	327
import rpz	328

ip-list	331
l2-bfd	331
l3-vlan-fwd-disable	333
lACP system-priority	334
lACP passthrough	334
ldap-server	335
link	336
lldp	338
locale	342
logging	343
mac-address	358
mac-age-time	359
maximum-paths	360
merge-mode-add	361
mirror-port	361
monitor	363
multi-config	365
multi-ctrl-cpu	365
netflow common max-packet-queue-time	369
netflow monitor	369
netflow template	376
netflow use-partition	380
no	381
ntp	381
object-group network	384
object-group service	386
offload-cpus	389
packet-handling	390
ping	390
poap	390
radius-server	391

raid	394
rba	394
resource-track	397
restore	399
route-map	400
router	405
router log file	406
router log log-buffer	407
run-hw-diag	408
running-config display	409
session-filter	410
sflow	411
smtp	415
snmp	417
so-counters	439
ssh-login-grace-time	441
sshd	442
syn-cookie	443
system	445
template	529
template ip-threat-action	531
tacacs-server host	532
tacacs-server monitor	534
techreport	535
terminal	536
tftp blksize	538
timezone	539
tx-congestion-ctrl	540
upgrade gui	540
upgrade hd	544
vcs	551

ve-stats	551
vlan	552
vlan-global enable-def-vlan-l2-forwarding	553
vlan-global l2-fwd-for-me-arp-ns	553
vlan-global l3-vlan-fwd-disable	554
web-service	554
write	559
Show Commands	559
show access-list	559
show acos-events messages	560
show active-partition	566
show admin	566
show aflex	572
show arp	573
show audit	574
show automatic-update	575
show axdebug capture	576
show axdebug config	577
show axdebug config-file	577
show axdebug file	578
show axdebug filter	580
show axdebug status	580
show backup	581
show bfd	582
show bootimage	590
show bpdu-fwd-group	591
show bridge-vlan-group	591
show bw-list	591
show class-list	593
show clns	595
show clock	596

show config	597
show config-block	597
show config-sync	598
show context	599
show core	600
show core-slots	600
show counters-all slb hm-dplane	601
show counters acos-events statistics	603
show counters acos-events collector-group	606
show counters drop error	606
show counters system ip-threat-list	607
show counters system session	609
show cpu	611
show debug	615
show disk	615
show dns cache	617
show dns-cache	627
show dns persistent-cache	627
show dns response-rate-limiting entries	629
show dns statistics	630
show dnssec	634
show dnssec dnskey	634
show dnssec ds	634
show dnssec statistics	635
show dnssec status	635
show dnssec template	635
show dumpthread	636
show environment	636
show errors	637
show event-action	640
show fail-safe	641

show file-system	644
show glid	648
show gui-image-list	649
show hardware	649
show health	651
show history	662
show icmp	662
show icmpv6	663
show interfaces	663
show interfaces brief	668
show interfaces media	670
show interfaces statistics	672
show interfaces transceiver	673
show ip	675
show ip anomaly-drop statistics	676
show ip bgp	681
show ip dns	682
show ip dns-cache	683
show ip fib show ipv6 fib	683
show ip fragmentation	684
show ip helper-address	689
show ip interfaces show ipv6 interfaces	694
show ip nat alg pptp	695
show ip nat interfaces show ipv6 nat interfaces	697
show ip isis show ipv6 isis	697
show ip nat pool show ipv6 nat pool	697
show ip nat pool-group show ipv6 nat pool-group	700
show ip nat range-list	700
show ip nat static-binding	701
show ip nat statistics	702
show ip nat template logging	702

show ip nat timeouts	703
show ip nat translations	703
show ip ospf show ipv6 ospf	705
show ip prefix-list show ipv6 prefix-list	705
show ip protocols show ipv6 protocols	705
show ip rip show ipv6 rip	705
show ip route show ipv6 route	706
show ip stats show ipv6 stats	707
show ip-list	708
show ipv6 ndisc	708
show ipv6 neighbor	710
show ipv6 traffic	711
show isis	712
show json-config	712
show json-config-detail	713
show json-config-with-default	714
show key-chain	715
show lacp	716
show lacp-passthrough	717
show license	718
show license-debug	718
show license-info	719
show lldp neighbor statistics	721
show lldp statistics	722
show locale	722
show local-log database	722
show local-uri-file	722
show log	723
show mac-address-table	724
show management	726
show memory	728

show mirror	731
show monitor	732
show netflow	733
show ntp	736
show pbslb	737
show pki	741
show poap	744
show process system	744
show radius-server	745
show reboot	745
show resource-accounting	746
show resource-tracked	750
show resource-tracked-by-user	751
show route-map	752
show router log file	753
show rpz	754
show run	755
show run visibility	757
show running-config	757
show session	760
show sflow	776
show shutdown	777
show smtp	777
show snmp engineID	777
show snmp oid	778
show snmp stats	782
show startup-config	783
show statistics	786
show store	787
show switch	788
show system app-performance	788

show system cpu-load-sharing	789
show system geo-location	791
show system ip-threat-list	795
show system inuse-rxtx-desc-info	796
show system inuse-rxtx-queue-info	797
show system job-offload statistics	797
show system link-monitor-polling-info	799
show system management-interface-mode	799
show system platform	800
show system path	801
show system port-list	803
show system radius server	803
show system radius table	805
show system rxtx-desc-info	806
show system rxtx-queue-info	807
show system resource-usage	807
show system shared-poll-mode	811
show system table-integrity	811
show system table-integrity statistics	812
show system tcp rate-limit-reset-unknown-conn	816
show system-ssl status	817
show tacacs-server	818
show techsupport	819
show terminal	822
show tftp	823
show trunk	823
show tsig	825
show version	825
show vlans	828
show vlan counter	829
show vlan counters	832

show vpn	833
clear dns cache	834
clear ip dns cache	837
clear system table-integrity	837
Application Delivery Partition	839
Configuration Commands	839
active-partition	839
application-type	840
partition	840
partition-admin	842
partition-group	846
service-partition	847
shared-vlan	849
Show Commands	855
show active-partition	855
show partition	855
show partition-config	857
show partition-group	858
ACOS Virtual Chassis System	859
Configuration Commands	859
device-context	859
vcs admin-session-connect	860
vcs database-distribution	862
vcs disable	862
vcs enable	863
vcs dead-interval	864
vcs dead-interval-mseconds	864
vcs debug	865
vcs device	866
vcs discovery-mode	868

vcs enable	870
vcs failure-retry-count	871
vcs floating-ip	872
vcs floating-ipv6	872
vcs force-wait-interval	873
vcs hold-preemption-interval	873
vcs multicast-ip	874
vcs multicast-ipv6	874
vcs multicast-port	875
vcs offload upgrade protocol <scp>	875
vcs reload	876
vcs ssl-enable	878
vcs time-interval	878
vcs time-interval-mseconds	879
vcs unicast-election	879
vcs vMaster-maintenance	881
vcs vmaster-take-over	882
Show Commands	883
show vcs debug	883
show vcs images	883
show vcs stat	885
show vcs summary	885
ACOS Virtual Router Redundant Protocol	889
Configuration Commands	889
migrate-vip	889
vrrp-a common	890
arp-retry	891
dead-timer	891
device-id	891
disable	892

disable-default-vrid	892
enable	893
forward-l4-packet-on-standby	893
get-ready-time	893
hello-interval	894
hostid-append-to-vrid	894
inline-mode	895
preemption-delay	896
restart-time	896
set-id	896
track-event-delay	897
vrrp-a fail-over-policy-template	897
vrrp-a force-self-standby	900
vrrp-a force-self-standby-persistent	900
vrrp-a interface	901
vrrp-a l2-inline-peer-ip	902
vrrp-a l3-inline-mode	903
vrrp-a ospf-inline	903
vrrp-a peer-group	904
vrrp-a preferred-session-sync-port ethernet	904
vrrp-a restart-port-list	905
vrrp-a vrid	906
vrrp-a vrid-lead	907
vrrp-a session-sync	908
vrrp-a vrid	908
blade-parameters	909
floating-ip	909
follow	910
preempt-mode	911
blade-parameters	912
fail-over-policy-template	912

priority	913
tracking-options	913
Show Commands	916
show vrrp-a	916
show vrrp-a all-partitions	921
show vrrp-a fail-over-policy-template	922
show vrrp-a hostid	923
show vrrp-a mac	923
show vrrp-a te-mac	924
show vrrp-a partition	924
show vrrp-a setid-monitor	925
show vrrp-a statistics	925
show vrrp-a vrid-lead	929
Scaleout	930
Configuration Commands	930
scaleout	930
scaleout apps enable	931
scaleout distributed-forwarding fw	931
scaleout distributed-forwarding slb	932
cgnv6 scaleout nat-ip-hashing-scheme	933
cluster-devices	933
local-device	934
id	934
l2-redirect	934
priority	935
session-sync	935
start-delay	936
tracking-template	936
traffic-redirection	938
service-config	939

user-group-count	939
match scaleout	940
Show Commands	941
show cgnv6 scaleout	941
show scaleout	942
show scaleout session-sync	948
show scaleout statistics	949
show scaleout traffic-map	957
show scaleout traffic-redirection	961
Carrier-Grade NAT	963
Configuration Commands	963
Large Scale NAT	963
class-list (for LSN)	963
cgnv6 enable-port-batch-v1	964
cgnv6 ecmp 4-tuple-hash	965
cgnv6 global domain-list	965
cgnv6 logging	967
cgnv6 lsn alg	970
cgnv6 lsn alg sip rtp-stun-timeout	971
cgnv6 lsn attempt-port-preservation	972
cgnv6 lsn endpoint-independent-filtering	972
cgnv6 lsn endpoint-independent-mapping	973
cgnv6 lsn enhanced-user-tracking	973
cgnv6 lsn hairpinning	974
cgnv6 lsn half-close-timeout	975
cgnv6 lsn health-check-gateway	975
cgnv6 lsn icmp	975
cgnv6 lsn inbound-refresh	976
cgnv6 lsn inbound-refresh-full-cone	976
cgnv6 lsn inside source class-list	977

cgnv6 lsn ip-selection	977
cgnv6 lsn logging default-template	978
cgnv6 lsn logging partition	979
cgnv6 lsn logging pool	980
cgnv6 lsn port-batching	980
cgnv6 lsn port-batching tcp-time-wait-interval	980
cgnv6 lsn port-overloading	981
cgnv6 lsn port-overloading allow-different-user	981
cgnv6 lsn port-overloading unique	982
cgnv6 lsn port-reservation	982
cgnv6 lsn strictly-sticky-nat	983
cgnv6 lsn stun-timeout	983
cgnv6 lsn syn-timeout	984
cgnv6 lsn tcp mss-clamp	984
cgnv6 lsn tcp reset-on-error	985
cgnv6 lsn-lid	985
cgnv6 lsn-radius-profile	990
cgnv6 lsn-rule-list	991
cgnv6 nat icmp always-source-nat-errors	1002
cgnv6 nat icmp respond-to-ping	1002
cgnv6 nat icmpv6 respond-to-ping	1002
cgnv6 nat inside source static	1003
cgnv6 nat inside source static partition	1003
cgnv6 nat pool	1003
cgnv6 nat pool-group	1006
cgnv6 nat range-list	1007
cgnv6 nat exclude-port	1008
cgnv6 one-to-one mapping-timeout	1009
cgnv6 one-to-one pool	1009
cgnv6 one-to-one pool-group	1010
cgnv6 port-list	1011

cgnv6 resource-usage	1012
cgnv6 sctp rate-limit	1013
cgnv6 template http-alg	1013
cgnv6 translation	1016
ip-list	1017
netflow monitor	1019
session-filter	1023
DNS64	1024
cgnv6 nat pool	1024
cgnv6 nat pool-group	1024
cgnv6 nat64 prefix	1024
cgnv6 server	1025
cgnv6 service-group	1026
cgnv6 template dns	1027
cgnv6 dns64-virtualserver	1034
NAT64	1035
cgnv6 ecmp 4-tuple-hash	1035
class-list (for NAT64)	1036
glid (for NAT64 override)	1037
cgnv6 nat pool (for NAT64)	1038
cgnv6 nat pool-group (for NAT64)	1038
cgnv6 lsn-lid	1038
cgnv6 nat64 alg	1039
cgnv6 nat64 force-non-zero-ipv4-id	1040
cgnv6 nat64 fragmentation df-bit-transparency	1041
cgnv6 nat64 fragmentation inbound	1041
cgnv6 nat64 fragmentation inbound df-set	1042
cgnv6 nat64 fragmentation outbound	1043
cgnv6 nat64 icmp	1043
cgnv6 nat64 inside	1044
cgnv6 nat64 prefix	1044

cgnv6 nat64 tcp mss-clamp	1045
cgnv6 nat64 tcp reset-on-error	1046
cgnv6 nat64 user-quota-prefix-length	1046
cgnv6 template policy	1046
ip nat inside	1048
ip nat-global reset-idle-tcp-conn	1049
ip frag timeout	1049
ip frag max-reassembly-sessions	1049
Dual-Stack Lite Commands	1050
class-list (for DS-Lite)	1050
cgnv6 ds-lite alg	1051
cgnv6 ds-lite fragmentation inbound	1051
cgnv6 ds-lite fragmentation outbound	1052
cgnv6 ds-lite icmp	1053
cgnv6 ds-lite inside source class-list	1054
cgnv6 ds-lite ip-checksum-error	1054
cgnv6 ds-lite l4-checksum-error	1055
cgnv6 ds-lite port-reservation	1055
cgnv6 ds-lite tcp mss-clamp	1056
cgnv6 ds-lite tcp reset-on-error	1057
cgnv6 ds-lite user-quota-prefix-length	1057
Port Control Protocol Commands	1059
cgnv6 pcp default-template	1059
cgnv6 template pcp	1060
Logging Template Commands	1063
cgnv6 template logging	1063
cgnv6 server	1083
cgnv6 service-group	1085
Fixed-NAT Command	1086
cgnv6 ecmp 4-tuple-hash	1086
cgnv6 lsn alg	1086

cgnv6 fixed-nat create-port-mapping-file	1087
cgnv6 fixed-nat port-mapping-files-count	1088
cgnv6 fixed-nat inside	1088
Stateless NAT46 Commands	1092
cgnv6 nat46-stateless fragmentation inbound	1092
cgnv6 nat46-stateless fragmentation outbound	1092
cgnv6 nat46-stateless fragmentation outbound df-set	1093
cgnv6 nat46-stateless partition-prefix	1093
cgnv6 nat46-stateless prefix	1093
cgnv6 nat46-stateless static-dest-mapping	1094
cgnv6 nat46-stateless tcp mss-clamp	1096
Lightweight 4over6 Commands	1098
class-list (for lw4o6)	1098
cgnv6 lw-4o6	1098
cgnv6 lw-4o6 binding-table	1099
cgnv6 lw-4o6 binding-table-validate	1100
cgnv6 lw-4o6 fragmentation inbound	1100
cgnv6 lw-4o6 fragmentation outbound	1101
cgnv6 lw-4o6 hairpinning	1102
cgnv6 lw-4o6 health-check-gateway	1103
cgnv6 lw-4o6 icmp-inbound	1103
cgnv6 lw-4o6 inside-src-access-list	1104
cgnv6 lw-4o6 nat-prefix-list	1104
cgnv6 lw-4o6 no-forward-match	1104
cgnv6 lw-4o6 no-reverse-match	1105
cgnv6 lw-4o6 save-binding-table	1106
cgnv6 lw-4o6 use-binding-table	1106
MAP Commands	1107
cgnv6 map encapsulation domain	1107
cgnv6 map encapsulation fragmentation inbound	1108
cgnv6 map encapsulation fragmentation outbound	1109

cgnv6 map translation domain	1110
cgnv6 map translation fragmentation inbound	1112
cgnv6 map translation fragmentation inbound df-set	1113
cgnv6 map translation fragmentation outbound	1113
NPTv6	1114
cgnv6 nptv6 domain	1114
cgnv6 nptv6 common send-icmpv6-on-error disable	1114
6rd Commands	1116
cgnv6 sixrd domain	1116
cgnv6 sixrd fragmentation inbound	1117
cgnv6 sixrd fragmentation outbound	1118
cgnv6 sixrd fragmentation outbound df-set	1119
DDoS Mitigation	1120
acos-application-only	1120
cgnv6 ddos-protection	1120
cgnv6 ddos-protection disable-nat-ip-by-bgp zone	1120
cgnv6 ddos-protection logging	1121
cgnv6 ddos-protection max-hw-entries	1121
cgnv6 ddos-protection packets-per-second	1121
cgnv6 ddos-protection packets-per-second ip	1123
cgnv6 ddos-protection syn-cookie	1127
cgnv6 lsn-lid conn-rate-limit	1128
ip anomaly-drop	1129
ip anomaly-drop ipv6-ext-header	1130
Show Commands	1134
clear cgnv6 ddos-protection disabled-ip-by-bgp	1134
clear cgnv6 ddos-protection ip-entries	1134
clear cgnv6 ddos-protection l4-entries	1134
clear cgnv6 ddos-protection statistics	1134
show cgnv6 ddos-protection disabled-ip-by-bgp	1135
show cgnv6 ddos-protection ip-entries	1135

show cgnv6 ddos-protection l4-entries	1136
show cgnv6 ddos-protection statistics	1137
show cgnv6 dns64 statistics	1137
show cgnv6 ds-lite alg	1139
show cgnv6 ds-lite full-cone-sessions	1139
show cgnv6 ds-lite inside-user	1141
show cgnv6 ds-lite nat-address	1144
show cgnv6 ds-lite port-reservations	1146
show cgnv6 ds-lite statistics	1147
show cgnv6 ds-lite user-quota-sessions	1151
show cgnv6 fixed-nat alg	1154
show cgnv6 fixed-nat full-cone-sessions	1155
show cgnv6 fixed-nat histogram	1156
show cgnv6 fixed-nat inside-user	1156
show cgnv6 fixed-nat nat-address	1157
show cgnv6 fixed-nat port-mapping-files	1157
show cgnv6 fixed-nat statistics	1158
show cgnv6 l4	1163
show cgnv6 logging keywords	1164
show cgnv6 logging source-address	1168
show cgnv6 logging statistics	1168
show cgnv6 logging tcp-svr-status	1171
show cgnv6 lsn alg	1172
show cgnv6 lsn enhanced-user-tracking	1178
show cgnv6 lsn full-cone-sessions	1180
show cgnv6 lsn inside-user	1182
show cgnv6 lsn nat-address	1184
show cgnv6 lsn port-overloading config	1186
show cgnv6 lsn port-reservations	1186
show cgnv6 lsn statistics	1187
show cgnv6 lsn system-status	1194

show cgnv6 lsn user-quota-sessions	1196
show cgnv6 lsn-lid	1198
show cgnv6 lsn-rule-list	1198
show cgnv6 lw-4o6 binding-table	1200
show cgnv6 lw-4o6 binding-table-validation-log files	1201
show cgnv6 lw-4o6 statistics	1201
show cgnv6 map encapsulation domain	1204
show cgnv6 map encapsulation statistics	1205
show cgnv6 map translation domain	1205
show cgnv6 map translation statistics	1205
show cgnv6 nat pool	1206
show cgnv6 nat pool-group	1211
show cgnv6 nat range-list	1212
show cgnv6 nat static-binding	1212
show cgnv6 nat46-stateless statistics	1212
show cgnv6 nat64 alg	1214
show cgnv6 nat64 conversion	1215
	1216
show cgnv6 nat64 enhanced-user-tracking	1216
show cgnv6 nat64 full-cone-sessions	1218
show cgnv6 nat64 inside-user	1220
show cgnv6 nat64 nat-address	1223
show cgnv6 nat64 prefixes	1225
show cgnv6 nat64 statistics	1225
show cgnv6 nat64 user-quota-sessions	1230
show cgnv6 nptv6	1233
show cgnv6 one-to-one mappings	1234
show cgnv6 one-to-one pool	1236
show cgnv6 one-to-one pool-group	1236
show cgnv6 one-to-one statistics	1236
show cgnv6 pcg statistics	1237

show cgnv6 resource-usage	1241
show cgnv6 sixrd statistics	1241
show cgnv6 template	1244
show counters cgnv6 fixed-nat hw-accelerate	1245
show counters cgnv6 fixed-nat per-instance	1247
show counters cgnv6 logging	1249
show counters cgnv6 lsn hw-accelerate	1252
show counters cgnv6 lsn per-instance	1254
show counters cgnv6 nat pool	1257
show counters cgnv6 nat64 hw-accelerate	1259
show ip anomaly-drop statistics	1261
show/clear lsn-alg esp	1263
show/clear nat64-alg esp	1264
Firewall	1265
Configuration Commands	1265
fw active-rule-set	1265
fw alg	1266
fw alg-processing	1268
fw allow-non-syn-session-create	1269
fw apply-changes	1270
fw clear-session-filter	1271
fw client class-list	1271
fw ddos-protection action	1273
fw ddos-protection dynamic-blacklist	1275
fw ddos-protection logging	1277
fw ddos-protection sampling-enable	1277
fw disable-application-category	1278
fw disable-application-metrics	1285
fw disable-application-protocol	1286
fw disable-ip-fw-sessions	1286

fw disable-undetermined-rule-logs	1287
fw dsr-mode-support	1287
fw extended-matching disable	1288
fw gtp apn-prefix-list	1289
fw gtp enable	1290
fw gtp insertion-mode apn-prefix-list	1290
fw gtp network-element-list-v4	1291
fw gtp network-element-list-v6	1292
fw gtp state-management	1293
fw hairpin next-hop-follow	1294
fw helper-sessions	1296
fw inbound-refresh	1297
fw inbound-refresh-full-cone	1297
fw listen-on-port-timeout	1298
fw local logging	1298
fw logging	1298
fw natip-ddos-protection	1300
fw permit-default-action	1300
fw respond-to-user-mac	1301
fw server	1302
fw service-group	1303
fw session-aging	1304
fw tcp mss-clamp	1308
fw tcp reset-on-error	1308
fw tcp-rst-close-immediate	1309
fw tcp syn-cookie	1310
fw tcp-window-check	1310
fw template logging	1311
fw urpf	1323
fw vrid	1324
object-group application	1325

rule-set	1325
remark	1326
rule	1327
rule-set rule action permit	1334
rule-set rule action-group permit	1336
rule-set rule action-group deny	1349
rule-set rule action-group reset	1350
sampling-enable	1351
application	1351
track-application	1352
session-statistic	1352
source	1353
dest	1354
system radius server	1355
template gtp	1360
template gtp-filter-list apn	1362
template gtp general-policy	1363
template gtp logging-policy	1364
template gtp msisdn-list	1365
template gtp rate-limit-policy	1365
template gtp-policy	1366
template limit-policy	1367
template limit-policy limit-pps	1373
template limit-policy limit-throughput	1375
template sctp	1377
traffic-control active-rule-set	1378
traffic-control rule-set	1379
remark	1379
rule	1380
zone	1385
Show Commands	1388

show automatic-update	1388
show counters fw alg	1388
show counters fw ddos-protection	1395
show counters fw global	1397
show counters fw gtp	1399
show counters fw hw-accelerate	1400
show counters fw logging	1402
show counters fw per-instance	1403
show counters fw rate-limit	1406
show counters fw server	1409
show counters fw service-group	1409
show counters fw tcp syn-cookie	1410
show counters fw tcp-window-check	1411
show counters rule-set	1411
show counters rule-set rule	1412
show counters sctp global	1414
show counters template gtp-policy	1415
show counters threat-intel threat-list	1418
show counters threat-intel webroot-global	1419
show fw application	1420
show fw ddos-protection entries	1422
show fw full-cone-sessions	1422
show fw limit-entry	1424
show fw logging-keywords	1425
show fw match	1427
show fw rate-limit	1428
show fw resource-usage	1432
show fw server	1434
show fw service-group	1435
show fw status	1437
show fw system-status	1439

show fw tcp syn-cookie statistics	1442
show fw top-k-rules	1443
show local-log database all/stats/file	1444
show rule-set	1446
show rule-set (application firewall)	1447
show sctp statistics	1455
show session application	1456
show session filter	1468
show session gtp	1476
show system radius server	1477
show system radius table	1478
show threat-intel database webroot	1480
show threat-intel ip-category	1482
show threat-intel log webroot	1482
show threat-intel hits webroot	1483
show traffic-control rule-set	1484
clear counters fw rate-limit	1485
clear counters threat-intel threat-list	1486
clear counters threat-intel webroot-global	1486
clear fw ddos	1486
clear fw ddos-protection	1487
clear fw full-cone-sessions	1487
clear fw tcp syn-cookie statistics	1487
clear fw top-k-rules	1487
clear sessions fw helper-sessions	1489
clear system radius server statistics	1489
clear system radius table	1489
clear tacacs-server statistics	1490
clear threat-intel hits webroot	1491

Next Generation Web Application Firewall	1492
Configuration Commands	1492
ng-waf	1492
license-manager ng-waf-module	1497
Show Commands	1498
clear ng-waf cache	1498
show ng-waf	1499
show ng-waf custom-page	1500
clear ng-waf custom-signals	1500
show ng-waf custom-signals	1500
show ng-waf status	1501
show ng-waf <virtual server> <port>	1504
Security Gateway	1512
Configuration Commands	1512
pki acme-cert	1512
account-email	1517
acme-client	1517
enroll	1518
log-level	1518
renew-before	1518
renew-every	1519
run-with-staging-server	1519
url	1520
pki acme-concurrent-process-count	1520
pki copy-cert	1521
pki copy-key	1522
pki cmp-cert	1523
cert-type	1523
cmp-ca	1524
cmp-cert	1524

log-level	1524
max-polltime	1525
recipient-dn	1525
renew-before	1525
renew-every	1526
secret	1526
subject-alternate-name	1527
pki create	1527
pki delete	1528
pki renew-self	1529
pki scep-cert	1530
dn	1530
enroll	1531
interval	1531
key-length	1531
log-level	1532
max-polltime	1532
method	1532
password	1533
renew-before	1533
renew-every	1533
subject-alternate-name	1534
san-domain	1534
system ipsec crypto-core	1534
system ipsec crypto-mem	1535
system ipsec fpga-decrypt	1535
system ipsec packet-round-robin	1535
vpn asymmetric-flow-support	1536
vpn extended-matching	1536
vpn fragment-after-encap	1536
vpn ike-logging-enable	1537

vpn ike-gateway	1537
auth-method	1537
configuration-payload	1539
dh-group	1539
dpd	1540
encryption	1541
interface-management	1543
ike-version	1543
key	1544
lifetime	1545
local-address	1545
local-cert	1545
local-id	1546
nat-traversal	1546
remote-address	1547
remote-ca-cert	1547
remote-id	1548
vrid	1548
radius-server	1549
vpn ike-acc-enable	1549
vpn ike-sa timeout	1550
vpn ike-stats-global	1550
vpn ipsec	1550
anti-replay-window	1551
bind	1552
crl	1552
dh-group	1552
dhcp-server	1553
disable	1554
disable-rekey	1554
domain	1554

enable	1554
encryption	1555
enroll	1557
force	1557
fragment-size	1557
ike-gateway	1558
lifebytes	1558
lifetime	1558
mode	1559
mtu	1559
proto	1560
sequence-number-disable	1560
speed	1560
traffic-selector	1560
up	1561
vpn ipsec-cipher-check	1562
vpn ipsec-group	1563
ipsec	1563
vpn jumbo-fragment	1564
vpn nat-traversal-flow-affinity	1564
vpn revocation	1565
ca	1565
ocsp	1565
vpn signature-authentication	1566
vpn stateful-mode	1566
vpn tcp-mss-adjust-disable	1567
Show Commands	1567
clear pki	1567
clear vpn cri	1568
clear vpn ike-sa	1568
clear vpn ike-stats	1568

clear vpn ike-stats-global	1569
clear vpn ipsec-group	1569
clear vpn ipsec-sa	1570
clear vpn log	1570
clear vpn ocsip	1570
debug monitor	1571
debug packet	1571
debug tunnel	1572
debug vpn level	1572
show counters-rate	1572
show counters vpn ike-gateway [NAME]	1574
show counters vpn ipsec [NAME]	1575
show hardware	1577
show vpn	1577
show vpn all-partitions	1578
show vpn partition <NAME>	1579
show vpn cri	1579
show vpn default	1580
show vpn ike-sa	1581
show vpn ike-sa-brief <NAME>	1583
show vpn ike-stats	1584
show vpn ike-stats-global	1585
show vpn ipsec-group	1587
show vpn ipsec-sa	1589
show vpn log	1592
show vpn ocsip	1592
Network Configuration	1594
Configuration Commands	1594
interface	1594
access-list	1597

bfd	1597
cpu-process	1600
dac-link-training-enable	1601
disable	1601
duplexity	1602
enable	1602
flow-control	1603
icmp-rate-limit	1603
icmpv6-rate-limit	1604
ip address	1606
ip address dhcp	1607
ip allow-promiscuous-vip	1608
ip cache-spoofing-port	1608
ip client	1609
ip control-apps-use-mgmt-port	1610
ip default-gateway	1611
ip helper-address	1612
ip igmp	1613
ip nat	1616
ip ospf	1617
ip rip authentication	1621
ip rip receive version	1622
ip rip receive-packet	1622
ip rip send version	1622
ip rip send-packet	1623
ip rip split-horizon	1623
ip router isis ipv6 router isis	1623
ip server	1624
ip slb-partition-redirect	1624
ip stateful-firewall	1625
ip ttl-ignore	1625

ipv6 (on management interface)	1626
ipv6 access-list	1626
ipv6 address	1627
ipv6 enable	1628
ipv6 nat inside	1628
ipv6 nat outside	1628
ipv6 ndisc router-advertisement	1629
ipv6 ospf cost	1633
ipv6 ospf dead-interval	1634
ipv6 ospf hello-interval	1634
ipv6 ospf mtu-ignore	1634
ipv6 ospf neighbor	1635
ipv6 ospf network	1636
ipv6 ospf priority	1636
ipv6 ospf retransmit-interval	1637
ipv6 ospf transmit-delay	1637
ipv6 rip split-horizon	1637
ipv6 router isis	1638
ipv6 router ospf	1638
ipv6 router rip	1639
ipv6 stateful-firewall	1639
ipv6 ttl-ignore	1639
isis authentication	1640
isis bfd	1641
isis circuit-type	1641
isis csnp-interval	1642
isis hello	1642
isis hello-interval	1643
isis hello-interval-minimal	1643
isis hello-multiplier	1644
isis lsp-interval	1645

isis mesh-group	1645
isis metric	1646
isis network	1646
isis password	1647
isis priority	1647
isis restart-hello-interval	1648
isis retransmit-interval	1649
isis wide-metric	1649
l3-vlan-fwd-disable	1650
lldp enable	1650
lldp notification	1651
lldp tx-dot1-tlvs	1651
lldp tx-tlvs	1651
load-interval	1652
lw-4o6	1652
map-inside	1653
map outside	1653
media-type-copper	1653
monitor	1654
mtu	1655
name	1656
ports-threshold	1656
remove-vlan-tag	1657
snmp-server	1658
traffic-distribution-mode	1659
trunk-group	1660
virtual-wire	1661
ip	1662
ip access-list	1663
ip address	1667
ip anomaly-drop	1668

ip as-path	1669
ip community-list	1670
ip large-community-list	1671
ip default-gateway	1672
ip dmz	1672
ip dns	1673
ip extcommunity-list	1674
ip frag buff	1674
ip frag cpu-threshold	1675
ip frag max-packets-per-reassembly	1675
ip frag max-reassembly-sessions	1676
ip frag timeout	1676
ip icmp disable	1677
ip-list	1677
ip map-list	1677
ip mgmt-traffic	1678
ip nat alg dns	1679
ip nat alg pptp	1680
ip nat icmp	1680
ip nat inside source	1680
ip nat pool	1682
ip nat pool-group	1684
ip nat range-list	1685
ip nat template logging	1687
ip nat translation	1690
ip nat-global reset-idle-tcp-conn	1691
ip prefix-list	1692
ip reroute	1695
ip route	1696
ip tcp syn-cookie threshold	1697
ipv4-in-ipv6 frag	1698

ipv6	1698
ipv6 access-list	1698
ipv6 address	1702
ipv6 default-gateway	1703
ipv6 frag timeout	1703
ipv6 icmpv6 disable	1704
ipv6 nat icmpv6 respond-to-ping	1704
ipv6 nat inside source list	1705
ipv6 nat pool	1705
ipv6 nat pool-group	1706
ipv6 neighbor	1707
ipv6 ospf display route single-line	1708
ipv6 prefix-list sequence-number	1709
iv6p reroute	1710
ipv6 route	1711
ipv6-in-ipv4 frag	1713
router	1713
router rip	1714
router ipv6 rip	1727
router ospf	1737
router ipv6 ospf	1749
router isis	1767
router bgp	1788
router bgp	1827
bgp extended-asn-cap	1827
bgp nexthop-trigger	1829
trunk-stats	1829
virtual-wire	1829
virtual-wire <number>	1829
virtual-wire-ethernet-group	1831
virtual-wire-global	1831

virtual-wire-health-check	1832
virtual-wire-vlan-pair	1840
virtual-wire-vlan-pair-set	1842
vlan	1843
name	1844
router-interface	1845
shared-vlan	1845
tagged	1846
traffic-distribution-mode	1846
untagged	1848
untagged lif	1849
Show Commands	1850
clear [ip] bgp {* AS-num}	1850
clear [ip] bgp external	1850
clear [ip] bgp ipv4	1851
clear [ip] bgp ipv4addr	1852
clear [ip] bgp ipv6	1852
clear [ip] bgp ipv6addr	1854
clear [ip] bgp peer-group	1854
clear [ip] bgp view	1855
clear ip rip route	1855
clear ipv6 rip route	1856
show [ip] bgp community	1856
show [ip] bgp community-list	1857
show [ip] bgp dampening	1857
show [ip] bgp filter-list	1858
show [ip] bgp inconsistent-as	1858
show [ip] bgp ipv4 {multicast unicast}	1858
show [ip] bgp paths	1861
show [ip] bgp prefix-list	1861
show [ip] bgp quote-regexp	1861

show [ip] bgp regexp	1861
show [ip] bgp route-map	1862
show [ip] bgp summary	1862
show {ip ipv6} ospf	1863
show {ip ipv6} ospf interface	1864
show {ip ipv6} ospf neighbor	1865
show {ip ipv6} ospf route	1866
show {ip ipv6} ospf virtual-links	1867
show bgp ipv4 neighbors	1868
show bgp ipv4 prefix-list	1869
show bgp ipv4 quote-regexp	1869
show bgp ipv4 summary	1870
show bgp ipv6	1870
show bgp ipv6addr	1873
show bgp nexthop-tracking	1873
show bgp nexthop-tree-details	1873
show ip bgp	1874
show ip bgp attribute-info	1875
show ip bgp cidr-only	1875
show ip bgp community-info	1875
show ip bgp ipv4addr	1875
show ip bgp scan	1876
show ip bgp view	1877
show ip isis [tag] route	1877
show ip ospf border-routers	1878
show ip ospf database	1879
show ip ospf redistributed	1881
show ip rip database	1883
show ip route acos	1884
show ipv6 isis [tag] route	1885
show ipv6 isis [tag] topology	1886

show ipv6 ospf database	1887
show ipv6 ospf topology	1889
show ipv6 rip database	1889
show isis [tag] database	1891
show isis [tag] topology	1892
show isis counter	1893
show isis interface	1895
show virtual-wire-global	1897
show virtual-wire-health-check	1898
Overlay Networks	1900
Configuration Commands	1900
debug packet	1900
interface lif	1902
overlay-mgmt-info	1902
overlay-tunnel vtep	1903
encap	1904
host	1905
local-ip-address	1906
remote-ip-address	1907
src-port-range	1910
vni	1911
overlay-tunnel options	1914
src-port-range	1917
Show Commands	1918
show interfaces brief	1918
show interfaces lif	1919
show overlay-tunnel	1920
show running-config overlay-mgmt-info	1922
show running-config overlay-tunnel	1923
show statistics interface	1924

show vlans	1925
Application Access Management	1926
Configuration Commands	1926
aam	1926
aam authentication	1927
aam authentication account	1927
aam authentication account kerberos-spn	1928
aam authentication account sampling-enable	1928
aam authentication global	1929
aam authentication jwt	1929
aam authentication log	1930
aam authentication log enable	1931
aam authentication log facility	1931
aam authentication logon	1931
aam authentication logon form-based	1932
aam authentication captcha	1936
aam authentication logon http-authenticate	1937
aam authentication portal	1938
aam authentication portal default-portal	1939
aam authentication relay	1946
aam authentication relay form-based	1947
aam authentication relay http-basic	1949
aam authentication relay kerberos	1950
aam authentication relay saml	1951
aam authentication relay ws-federation	1952
aam authentication saml	1953
aam authentication saml identity-provider	1953
aam authentication saml service-provider	1954
aam authentication server	1957
aam authentication server ldap	1957

aam authentication server oosp	1960
aam authentication server radius	1961
aam authentication server windows	1962
aam authentication service-group	1964
aam authentication template	1965
aam authorization policy	1968
aam authentication oauth authorization-server	1971
aam authentication oauth client	1972
aam authentication relay oauth	1973
aam aaa-policy	1973
access-list	1974
action	1974
authentication-template	1975
authorize-policy	1975
captcha-authz-policy	1976
domain-name	1976
host	1977
match-encoded-uri	1977
port	1978
uri	1978
Show Commands	1979
clear aam authentication kcache	1979
clear aam authentication rdns	1979
clear aam authentication service-group	1979
clear aam authentication session	1979
clear aam authentication statistics	1980
clear aam authentication statistics jwt	1981
clear aam authorization jwt cache	1981
clear aam authentication saml idp status	1981
show aam aaa-policy	1982
show aam authentication	1982

show aam authentication account	1982
show aam authentication default-portal	1984
show aam authentication jwks	1984
show aam authentication klist	1985
show aam authentication logon	1987
show aam authentication logon form-based	1987
show aam authentication logon http-authenticate	1988
show aam authentication portal	1989
show aam authentication portal-image	1989
show aam authentication relay	1989
show aam authentication saml	1990
show aam authentication server	1990
show aam authentication service-group	1991
show aam authentication session	1992
show aam authentication session-attributes	1994
show aam authentication session-with-attributes	1994
show aam authentication statistics	1995
show aam authentication statistics captcha	2007
show aam authentication statistics jwt	2008
show aam authentication template	2008
show aam authorization jwt cache	2008
show aam authorization policy	2009
Global Server Load Balancing	2010
Configuration Commands	2010
delete geo-location	2010
gslb active-rdt	2011
gslb dns action	2012
gslb dns logging	2013
gslb geo-location	2014
gslb group	2015

gslb ip-list	2019
gslb policy	2020
active-rdt	2021
active-servers	2025
active-servers-enable	2026
admin-ip	2026
admin-ip-enable	2027
admin-preference	2027
alias-admin-preference	2028
auto-map	2028
bw-cost	2029
bw-cost-enable	2030
capacity	2030
connection-count-by-site	2031
connection-load	2032
dns action	2034
dns active-only	2034
dns addition-mx	2036
dns auto-map	2036
dns backup-alias	2037
dns backup-server	2038
dns cache	2038
dns cname-detect	2040
dns delegation	2041
dns external-ip	2041
dns external-soa	2042
dns geoloc-action	2043
dns geoloc-alias	2044
dns geoloc-policy	2045
dns hint	2046
dns ip-replace	2047

dns ipv6 mapping	2048
dns ipv6 mix	2050
dns ipv6 smart	2051
dns logging	2051
dns proxy block <query>	2053
dns proxy block <type>	2054
dns proxy block action	2056
dns selected-only	2057
dns server	2058
dns sticky	2061
dns sticky option	2063
dns ttl	2065
edns client-subnet geographic	2066
geo-location	2068
geo-location-match	2069
geographic	2071
health-check	2071
ip-list	2072
least-response	2072
metric-fail-break	2073
metric-force-check	2073
metric-order	2073
num-session	2074
num-session-enable	2076
round-robin	2076
weighted-alias	2077
weighted-ip	2078
weighted-ip-enable	2079
weighted-site	2079
weighted-site-enable	2080
dns server	2080

gslb protocol	2081
gslb protocol limit	2083
gslb secure-attributes	2084
gslb service-group	2086
gslb service-ip	2087
gslb service-matching-rules	2091
gslb site	2095
gslb sync-objects	2102
gslb system age-interval	2103
gslb system auto-map module	2104
gslb system auto-map ttl	2105
gslb system geo-location load	2105
gslb system ip-ttl	2106
gslb system wait	2106
gslb template csv	2107
gslb template snmp	2108
gslb zone	2111
import geo-location	2124
ip dns	2125
Show Commands	2126
show counters gslb dns	2126
show domain-list	2127
show gslb cache	2128
show gslb config	2129
show gslb fqdn	2132
show gslb geo-location	2132
show gslb group	2137
show gslb ip-list	2142
show gslb memory	2143
show gslb policy	2144
show gslb protocol	2144

show gslb rdt	2148
show gslb samples conn	2152
show gslb samples conn-load	2153
show gslb samples rdt	2155
show gslb service	2156
show gslb service-group	2158
show gslb service-ip	2159
show gslb service-port	2160
show gslb session	2161
show gslb site	2163
show gslb slb-device	2167
show gslb state	2169
show gslb statistics	2169
show gslb statistics secure	2171
show gslb zone	2172
clear gslb	2177

Server Load Balancing 2179

Configuration Commands	2179
health monitor	2179
default-state-up	2179
disable-after-down	2180
dsr-l2-strict	2180
header-insert	2181
health external	2181
interval	2183
method	2184
override-ipv4	2202
override-ipv6	2203
override-port	2203
passive	2204

proxy-header	2206
retry	2207
server-ssl	2208
ssl-ciphers	2209
ssl-ticket	2210
ssl-ticket lifetime	2210
ssl-version	2211
strictly-retry-on-server-error-response	2212
up-retry	2212
slb common	2213
aflex-table-entry-aging-interval	2213
aflex-table-entry-sync	2214
ecmp-hash	2215
low-latency	2215
service-group-on-no-dest-nat-vports	2216
buff-thresh	2217
cert-pinning	2218
compress-block-size	2219
conn-rate-limit src-ip	2220
ddos-protection	2222
ddos-protection logging	2222
ddos-protection packets-per-second	2223
disable-adaptive-resource-check	2223
disable-persist-scoring	2224
disable-server-auto-reselect	2224
dns-cache-age	2225
dns-cache-age-min-threshold	2226
dns-cache-aging-weight	2227
dns-cache-enable	2227
dns-cache-entry-size	2229
dns-cache-sync	2230

dns-cache-sync-entry-size	2230
dns-cache-sync-ttl-threshold	2231
dns-cache-ttl-adjustment-enable	2231
dns-cache-hitcount-enable	2232
dns-cookie-cache-policy	2232
dns-negative-cache-enable	2233
dns-negative-cache-bypass-threshold	2234
dns-persistent-cache-enable	2234
dns-persistent-cache-hit-threshold	2235
dns-persistent-cache-ttl-threshold	2235
dns-response-rate-limiting	2236
dns-vip-stateless	2237
drop-icmp-to-vip-when-vip-down	2237
dsr-health-check-enable	2238
ecmp-hash	2238
enable-l7-req-acct	2239
extended-stats	2240
fast-path-disable	2240
gateway-health-check	2240
global-dns-cache	2241
graceful-shutdown	2245
honor-server-response-ttl	2245
hw-compression	2246
hw-syn-rr	2246
lb-method-hash	2247
l2l3-trunk-lb-disable	2249
max-buff-queued-per-conn	2250
max-http-header-count	2250
max-persistent-cache	2250
msl-time	2251
mss-table	2252

ng-waf	2252
no-auto-up-on-aflex	2258
odd-even-nat-enable	2258
pbslb-entry-age	2259
rate-limit-logging	2260
recursive-ns-cache	2261
reset-stale-session	2262
scale-out	2262
service-group-on-no-dest-nat-vports	2263
snat-gwy-for-l3	2263
snat-on-vip	2264
sort-res	2265
ssl-module	2267
ssli-sni-hash-enable	2269
ssli-silent-termination-enable	2272
stateless-sg-multi-binding	2273
stats-data-disable	2273
use-mss-tab	2274
slb forward-proxy	2274
slb resource-usage	2277
slb resource-usage threshold	2282
slb server	2283
support-http2	2285
alternate	2286
conn-limit	2287
conn-resume	2287
disable	2288
disable-with-health-check	2289
enable	2290
extended-stats	2290
external-ip	2290

health-check	2291
health-check-disable	2291
ipv6	2291
port	2292
slow-start	2298
spoofing-cache	2299
stats-data-disable	2299
stats-data-enable	2299
template server	2300
weight	2300
slb service-group	2301
backup-server-event-log	2303
extended-stats	2305
health monitor	2305
health-check-disable	2306
member	2306
method	2310
min-active-member	2320
persist-scoring	2322
priority	2323
priority-affinity	2325
reset auto-switch	2326
reset-on-server-selection-fail	2326
sample-rsp-time	2326
stats-data-disable	2327
stats-data-enable	2327
strict-select	2327
template	2328
traffic-replication-type	2329
slb ssl	2331
slb ssl-cert-revoke sampling-enable	2331

slb ssl-expire-check email-address	2333
slb ssl-expire-check exception	2333
slb ssl-forward-proxy sampling-enable	2334
slb svm-source-nat pool	2335
slb template	2335
slb template cache	2336
accept-reload-req	2337
age	2338
default-policy-nocache	2338
disable-insert-age	2339
disable-insert-via	2339
max-cache-size	2339
max-content-size	2340
min-content-size	2341
packet-capture-template	2341
policy	2341
remove-cookies	2342
replacement-policy LFU	2343
template logging	2343
verify-host	2344
slb template cipher	2344
slb template connection-reuse	2346
slb template dblb	2348
slb template diameter	2349
slb template dns	2354
add-padding-to-client	2355
cache-hitcount-enable	2356
cache-record-serving-policy	2356
cache-ttl-adjustment-enable	2357
category-lookup	2358
category-lookup-bypass	2359

category-lookup-online-lookup	2360
class-list	2360
default-policy	2361
disable-dns-template	2361
disable-ra-cached-resp	2362
disable-rpz-attach-soa	2362
dns-cookie-cache-policy	2362
dns-log-enable	2363
dns64	2364
dnssec-service-group	2366
enable-cache-sharing	2367
insert-client-subnet	2367
malformed-query	2368
max-cache-entry-size	2369
max-cache-size	2369
max-query-length	2370
negative-dns-cache enable	2371
query-class-filter	2372
query-id-switch	2374
query-rate-monitoring	2374
query-type-filter	2375
recursive-dns-resolution	2377
redirect-to-tcp-port	2383
remove-aa-flag	2384
remove-edns-csubnet-to-server	2384
remove-padding-to-server	2384
response-rate-limiting	2385
rpz	2389
template	2390
tld-filter-log-enable	2390
tld-filter-white-list	2391

udp-retransmit	2391
slb template dns-logging	2392
slb template doh	2403
slb template dynamic-service	2408
slb template external-service	2410
slb template fix	2413
slb template ftp	2415
slb template http	2416
slb template http-policy	2437
slb template imap-pop3	2445
slb template link-block-as-down	2446
slb template link-cost	2447
slb template link-down-on-restart	2448
slb template link-probe	2449
destination hostname	2449
destination hostname target	2450
expected-status-code	2451
probe-interval	2452
probes-per-test	2452
rtt-method	2453
selection-rule	2454
test-interval	2454
url	2455
user-tag	2455
slb template logging	2456
slb template mqtt	2457
slb template monitor	2459
slb template persist cookie	2461
slb template persist destination-ip	2467
slb template persist source-ip	2471
slb template persist ssl-sid	2476

slb template policy	2477
acos-event-log	2480
action	2480
bw-list id	2482
bw-list name	2483
bw-list over-limit	2483
bw-list timeout	2484
bw-list use-destination-ip	2485
bw-rate-limit	2485
class-list	2486
conn-limit	2487
conn-rate-limit	2488
forward-policy	2488
forward-policy ssli-url-filtering	2512
forward-policy ssli-url-filtering-san	2513
geo-location full-domain-tree	2514
geo-location overlap	2515
geo-location share	2515
over-limit-action	2516
request-limit	2517
request-rate-limit	2517
response-code-rate-limit	2518
slb template port	2519
bw-rate-limit	2520
conn-limit	2521
conn-rate-limit	2521
dampening-flaps	2522
del-session-on-server-down	2523
dest-nat	2524
down-grace-period	2524
dscp	2525

dynamic-member-priority	2526
extended-stats	2527
health-check	2527
health-check-disable	2528
inband-health-check	2528
no-ssl	2530
request-rate-limit	2530
slow-start	2531
source-nat	2532
stats-data-disable	2533
stats-data-enable	2533
weight	2534
slb template quic	2535
slb template reqmod-icap	2537
allowed-http-methods	2538
disable-http-server-reset	2539
fail-close	2540
include-protocol-in-uri	2540
log-only-allowed-method	2540
min-payload-size	2541
preview	2541
service-group	2542
service-url	2543
template	2543
slb template respmod-icap	2544
disable-http-server-reset	2545
fail-close	2545
include-protocol-in-uri	2545
log-only-allowed-method	2546
min-payload-size	2546
preview	2547

service-group	2547
service-url	2548
template	2548
slb template server	2549
bw-rate-limit	2550
bw-rate-limit-acct	2551
conn-limit	2551
conn-rate-limit	2552
dns-query-interval	2553
dynamic-server-prefix	2554
extended-stats	2554
health-check	2554
health-check-disable	2555
l2-health-check-path	2555
log-selection-failure	2556
max-dynamic-server	2556
min-ttl-ratio	2557
slow-start	2557
spoofing-cache	2559
stats-data-disable	2559
stats-data-enable	2560
support-http2	2560
weight	2561
slb template sip (over TCP/TLS)	2562
alg-dest-nat	2562
alg-source-nat	2563
call-id-persist-disable	2563
client-keepalive	2563
client-request-header erase	2564
client-request-header insert	2564
client-response-header erase	2565

client-response-header insert	2566
dialog-aware	2567
exclude-translation	2567
failed-client-selection	2568
failed-server-selection	2568
insert-client-ip	2569
server-keep-alive	2569
server-request-header erase	2570
server-request-header insert	2570
server-response-header erase	2571
server-response-header insert	2572
server-selection-per-request	2573
smp-call-id-rtp-session	2573
timeout	2574
slb template sip (over UDP)	2575
alg-dest-nat	2575
alg-source-nat	2576
call-id-persist-disable	2576
client-request-header erase	2577
client-request-header insert	2577
client-response-header erase	2578
client-response-header insert	2578
dialog-aware	2579
exclude-translation	2580
insert-client-ip	2580
keep-server-ip-if-match-acl	2581
registrar service-group	2581
server-request-header erase	2582
server-request-header insert	2582
server-response-header erase	2583
server-response-header insert	2583

timeout	2584
slb template smpp	2585
client-enquire-link	2585
server-enquire-link	2586
server-selection-per-request	2586
user	2587
slb template smtp	2587
client-domain-switching	2589
command-disable	2590
server-domain	2591
service-ready-msg	2591
starttls	2592
slb template tcp	2593
del-session-on-server-down	2594
force-delete-timeout	2594
force-delete-timeout-100ms	2595
half-open-idle-timeout	2596
idle-timeout	2596
initial-window-size	2597
insert-client-ip	2598
lan-fast-ack	2598
proxy-header	2599
qos	2600
reset-follow-fin	2600
reset-fwd	2601
reset-rev	2601
slb template tcp-proxy	2602
proxy-header	2603
ack-aggressiveness	2604
backend-wscale	2605
del-session-on-server-down	2605

disable-abc	2606
disable-sack	2606
disable-tcp-timestamps	2607
disable-window-scale	2607
do-newsack	2607
dynamic-buffer-allocation	2608
early-retransmit	2608
fin-timeout	2609
force-delete-timeout	2610
force-delete-timeout-100ms	2610
half-close-idle-timeout	2611
half-open-idle-timeout	2611
idle-timeout	2612
init-cwnd	2613
initial-window-size	2613
insert-client-ip	2614
invalid-rate-limit	2615
keepalive-interval	2615
keepalive-probes	2617
limited_slowstart	2617
maxburst	2618
min-rto	2618
mss	2619
nagle	2619
naked-ack-on-handshake	2620
psh-flag-optimization	2620
qos	2621
reassembly-limit	2621
reassembly-timeout	2622
receive-buffer	2622
reno	2623

reset-fwd	2623
reset-rev	2623
retransmit-retries	2624
syn-retries	2625
timewait	2625
transmit-buffer	2626
slb template udp	2626
aging	2627
idle-timeout	2628
qos	2629
radius-lb-method	2630
re-select-if-server-down	2631
stateless-conn-timeout	2632
slb template virtual-port	2632
aflow	2634
allow-syn-otherflags	2635
allow-vip-to-rport-mapping	2636
conn-limit	2636
conn-rate-limit	2637
drop-unknown-conn	2638
dscp	2639
ignore-tcp-msl	2640
non-syn-initiation	2640
pkt-rate-limit	2641
reset-l7-on-failover	2642
reset-unknown-conn	2643
snat-msl	2643
snat-port-preserve	2644
slb template virtual-server	2645
conn-limit	2646
conn-rate-limit	2647

disable-when-all-ports-down	2648
disable-when-all-ports-down	2648
icmp-rate-limit	2649
icmpv6-rate-limit	2649
subnet-gratuitous-arp	2650
support-http2	2651
template server-ssl	2652
slb transparent-acl-template	2652
slb transparent-tcp-template	2653
slb virtual-server	2654
template client-ssl	2656
template server	2657
arp-disable	2658
description	2658
disable	2658
disable-when-all-ports-down	2659
disable-when-any-port-down	2659
enable	2660
extended-stats	2660
port	2660
redistribution-flagged	2664
stats-data-disable	2664
stats-data-enable	2665
template logging	2665
template policy	2665
template scaleout	2665
template virtual-server	2666
vrid	2666
slb virtual-server port	2668
aflex-table-entry-sync	2668
attack-detection	2668

aaa-policy	2669
access-list	2669
aflex	2671
alternate	2671
bucket-count	2672
clientip-sticky-nat	2672
conn-limit	2673
def-selection-if-pref-failed	2674
def-selection-if-pref-failed-disable	2676
disable	2676
enable	2676
extended-stats	2676
force-routing-mode	2677
gslb-enable	2677
ha-conn-mirror	2677
ipinip	2678
ip-map-list	2679
message-switching	2679
name	2679
no-auto-up-on-aflex	2679
no-dest-nat	2680
optimization-level	2681
rate-limit-pr-log	2683
redirect-fwd	2683
redirect-rev	2683
redirect-to-https	2684
reply-acme-challenge	2684
reset-on-server-selection-fail	2685
rtp-sip-call-id-match	2685
service-group	2686
skip-rev-hash	2687

snat-on-vip	2687
source-nat auto	2688
source-nat pool	2692
source-nat use-cgnv6	2692
stats-data-disable	2693
stats-data-enable	2693
support-http2	2693
syn-cookie	2694
template	2695
template virtual-port	2696
template quic	2697
use-default-if-no-server	2698
use-rcv-hop-for-resp	2698
when-server-selection-failed	2700
Show Commands	2701
show dns cache rate	2701
show hardware-accelerate slb statistics	2702
show hardware-accelerate statistics	2704
show hardware-accelerate status	2705
show hardware-forward slb statistics	2706
show hardware-forward statistics	2707
show hardware-forward status	2708
show run slb template	2708
show slb	2710
show slb aflow	2719
show slb attack-prevention	2719
show slb cache	2720
show slb common	2728
show slb compression	2729
show slb connection-reuse	2729
show slb conn-rate-limit	2731

show slb ddos-protection l4-entries	2733
show slb ddos-protection statistics	2734
show slb dns-custom-logging-keywords	2735
show slb diameter	2736
show slb fast-fix	2742
show slb fast-http-proxy	2743
show slb fix	2746
show slb forward-policy-source-port-translation-only-stats	2748
show slb ftp	2748
show slb ftp-proxy	2749
show slb generic-proxy	2750
show slb geo-location	2750
show slb http-proxy	2752
show slb http3	2764
show slb hw-compression	2776
show slb icap	2777
show slb icap-http	2779
show slb imap-proxy	2783
show slb l4	2786
show slb l7session	2800
show slb link-probe	2801
show slb mlb	2806
show slb mssql	2807
show slb mqtt	2809
show slb mysql	2811
show slb passthrough	2813
show slb persist	2814
show slb player-id-check-status	2817
show slb player-id-records-all	2817
show slb player-id-stats	2818
show slb pop3-proxy	2819

show slb quic	2820
show slb rate-limit-for-reset-unknown-conn	2838
show slb rate-limit-logging	2839
show slb resource-usage	2841
show slb server	2843
show slb service-group	2860
show slb sip	2868
show slb smpp	2870
show slb smtp	2877
show slb source-port-rate-limit	2880
show slb spdy-proxy	2881
show slb sshi	2884
show slb switch	2884
show slb syn-cookie	2892
show slb syn-cookie-buffer	2892
show slb tcp stack	2892
show slb template policy forward-policy-stats	2894
show slb virtual-server	2897
clear health https ssl-ticket	2938
clear slb unused-server-ports	2939
clear slb virtual-server	2940
Secure Socket Layer Insight	2944
Configuration Commands	2944
slb template client-ssl	2944
auth-username	2946
auth-username-attribute	2947
authorization	2948
ca-cert	2949
certificate	2950
cipher	2951

client-certificate	2951
client-certificate-Request-CA	2952
close-notify	2953
crl	2954
dh-param	2955
direct-client-server-auth	2955
disable-sslv3	2955
early-data	2956
ec-name	2957
enable-ssli-ftp-alg	2959
enable-tls-alert-logging fatal	2959
forward-proxy-alt-sign cert	2960
forward-proxy-block-message	2961
forward-proxy-bypass ad-group-list	2961
forward-proxy-bypass case-insensitive	2962
forward-proxy-bypass central-cert-pin-list	2963
forward-proxy-bypass certificate-issuer	2964
forward-proxy-bypass certificate-san	2965
forward-proxy-bypass certificate-subject	2967
forward-proxy-bypass class-list	2969
forward-proxy-bypass client-auth	2970
forward-proxy-bypass client-ip-list	2972
forward-proxy-bypass contains	2973
forward-proxy-bypass ends-with	2974
forward-proxy-bypass equals	2975
forward-proxy-bypass exception-ad-group-list	2976
forward-proxy-bypass exception-class-list	2977
forward-proxy-bypass exception-client-ip-list	2977
forward-proxy-bypass exception-server-ip-list	2979
forward-proxy-bypass exception-user-name-list	2980
forward-proxy-bypass exception-web-category	2981

forward-proxy-bypass exception-web-reputation	2982
forward-proxy-bypass local-cert-pin-list	2983
forward-proxy-bypass require-web-category	2984
forward-proxy-bypass starts-with	2985
forward-proxy-bypass server-ip-list	2986
forward-proxy-bypass web-category	2987
forward-proxy-bypass web-reputation	2988
forward-proxy-ca-certificate	2989
forward-proxy-cache-persistence	2990
forward-proxy-cert-cache	2991
forward-proxy-cert-expiry	2992
forward-proxy-cert-ext	2992
forward-proxy-cert-not-ready-action	2993
forward-proxy-cert-revoke-action	2993
forward-proxy-cert-unknown-action	2994
forward-proxy-cert-validity	2996
forward-proxy-crl-disable	2996
forward-proxy-decrypted	2997
forward-proxy-enable	2997
forward-proxy-esni-action	2998
forward-proxy-failsafe-disable	2998
forward-proxy-inspect	2999
forward-proxy-inspect certificate-issuer	3000
forward-proxy-inspect certificate-san	3001
forward-proxy-inspect certificate-subject	3002
forward-proxy-log-disable	3002
forward-proxy-no-shared-cipher-action	3003
forward-proxy-no-sni-action	3003
forward-proxy-ocsp-disable	3004
forward-proxy-require-sni-cert-matched	3004
forward-proxy-selfsign-redir	3005

forward-proxy-source-nat	3005
forward-proxy-ssl-version	3006
forward-proxy-trusted-ca	3007
forward-proxy-verify-cert-fail-action	3008
handshake-logging-enable	3008
hsm-param	3009
ja3-enable	3009
ja3-insert-http-header	3009
ja3-reject-class-list	3010
ja3-reject-max-number-per-host	3011
ja4-enable	3012
ja4-insert-http-header	3013
ja4-reject-class-list	3013
ja4-reject-max-number-per-host	3014
local-logging	3015
non-ssl-bypass	3016
ocsp-stapling	3016
renegotiation-disable	3017
require-sni-cert-matched	3017
server-name	3018
server-name-auto-map	3019
server-name-regex	3020
server-name-bypass	3022
session-cache-size	3023
session-cache-timeout	3024
session-key-logging-enable	3024
session-ticket-disable	3024
session-ticket-lifetime	3025
ssl-false-start-disable	3025
ssli-inbound-enable	3026
ssli-logging	3027

ssl2-bypass	3028
template	3028
version	3029
slb template client-ssh	3030
forward-proxy-enable	3031
slb template server-ssl	3031
ca-cert	3034
certificate	3035
cipher	3035
close-notify	3036
crl	3037
dh-param	3037
early-data	3038
ec-name	3038
enable-ssli-ftp-alg	3039
enable-tls-alert-logging fatal	3039
forward-proxy-enable	3039
handshake-logging-enable	3040
ocsp-stapling	3040
renegotiation-disable	3040
server-certificate-error	3041
server-name	3042
session-cache-size	3042
session-cache-timeout	3042
session-key-logging-enable	3043
session-ticket-enable	3043
ssli-logging	3044
template cipher	3044
use-client-sni	3045
version	3045
slb template server-ssh	3046

forward-proxy-enable	3047
slb template ssli	3047
type	3048
web-category	3048
Show Commands	3058
show slb ssl	3058
show slb ssl-cert-revoke-stats	3070
show slb ssl-counters	3073
show slb ssl-crl	3083
show slb ssl-cert-pinning-candidate-list	3088
show slb ssl-cert-pinning-candidate-list central-list	3090
show slb ssl-cert-pinning-candidate-list local-list	3092
show slb ssl-expire-check	3094
show slb ssl-forward-proxy-cert	3094
show slb ssl-forward-proxy-stats	3098
show slb ssl-ja3	3100
show slb ssl-ja4	3100
show slb ssl-ocsp cache	3101
show slb ssl-ocsp cache detail	3102
show web-category	3105
show web-reputation	3113
Cloud Services	3115
Configuration Commands	3115
cloud-services	3115
cloud-services cloud-provider	3116
cloud-services cloud-provider aws	3117
cloud-services cloud-provider aws log	3119
cloud-services cloud-provider aws metrics	3120
cloud-services cloud-provider aws multi-az-failover	3125
cloud-services cloud-provider azure	3128

cloud-services cloud-provider azure log 3129

cloud-services cloud-provider azure metrics 3131

cloud-services cloud-provider vmware 3138

cloud-services cloud-provider vmware log 3139

cloud-services cloud-provider vmware metrics 3141

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}
<i>Italics</i> <i>with or without angle brackets <></i>	Indicates the required parameter for which you must supply a value.	[no] user-tag <i><name></i> [no] partition-group <i>group-name</i>
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 <i>partition-admin-username</i> [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>	Help	Displays the CLI Quick Reference
or ACOS#	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.
or (config) #	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 <i>string</i>	Begins the output with the line containing the specified string.
include <i>string</i>	Displays only the output lines that contain the specified string.
exclude <i>string</i>	Displays only the output lines that <i>do not</i> contain the specified string.
section <i>string</i>	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] <i>string</i>	Display only those lines matching the specified <code>grep</code> expression. NOTE: If the <code>grep</code> expression matches the same letters as “invert-match” the command will fail since the CLI will not be able to distinguish between the <code>invert-match</code> option and a desired <code>grep</code> patten. To work around this issue, enclose the desired <code>grep</code> expression in quotation marks. For example, the following command would be invalid: <pre>show log grep in</pre> However, the following would return the desired result:

Table 6 : show log Command Output Additional Filters

Filter	Description
	<code>show log grep "in"</code>
awk <code>[fsseparator]</code> print <code>expression</code>	Displays only the fields matching the specified awk expression. NOTE: When specifying multiple expressions, use quotation 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: <code>show log awk fs : print \$1,\$2</code> <code>show log awk fs : print "\$1, \$2"</code>
cut <code>[</code> <code>delimiterchar</code> <code>fieldsfield</code>	Do not show the output matching the specified cut expression.
sort <code>[numeric-sort]</code> <code>[reverse]</code> <code>[unique]</code>	Sort the lines in the output based on the specified sort expression.
uniq <code>[skip-charsnum]</code> <code>[skip-fieldsnum]</code> <code>[count]</code> <code>[repeated]</code>	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>
```

- AX Series models contain “AX” plus the model number in the prompt. For example, when an EXEC session is started, the AX Series 5630 will display the following prompt:

```
AX5630>
```

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 or AX Series devices 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 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-con-fig	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 .
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 .
save-con-fig	Use this command to save the axDebug configuration to a file. For more information, see save-config .

Parameter	Description
<code>sess-filter-dis</code>	Use this command to disable session based filter. For more information, see sess-filter-dis .
<code>tcpdump</code>	Use this command to display and filter packets. For more information, see tcpdump .
<code>timeout</code>	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 <i>filename</i> [<i>max-packets</i>] [incoming [portnum ...]] [outgoing [portnum ...]]	Saves captured packets in a file: • <i>filename</i> – Specifies the name of the packet capture file. • <i>max-packets</i> – 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 : 1U.<..?....-
Y....
0xa6657098: 00000000 00000000 00000000 00000000 :
.....
o( 3, 0, ccaf)> 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 : 1U.<..?....-
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
```

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 <i>ipaddr</i> mac <i>macaddr</i> port <i>portnum</i> }	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 <i>ipaddr</i> { <i>subnet-mask</i> <i>/mask-length</i> }	Matches on the specified IPv4 address.
mac <i>macaddr</i>	Matches on the specified MAC address.
offset <i>position</i>	Matches on the specified length of bytes

Command	Description
length <i>bytes</i> <i>operator value</i>	and value of those bytes within the packet: <i>position</i> – Starting position within the packet, 0-65535 bytes. <i>bytes</i> – Number of consecutive bytes to filter on, from 0-65535, beginning at the offset position. <i>operator</i> – One of the following: > (greater than) >= (greater than or equal to) <= (smaller than or equal to) < (smaller than) = (equal to) range <i>min-value max-value</i> (select a range) <i>value</i> – String to filter on.
port <i>min-portnum</i> <i>max-portnum</i>	Matches on the specified range of protocol port numbers.
proto { icmp icmpv6 tcp udp <i>portnum</i> }	Matches on the specified protocol or protocol port number.
src { ip <i>ipaddr</i> mac <i>macaddr</i> port <i>port-num</i> }	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
pcapng-enable	Enables capturing files in the .pcapng format.
ssl-key-enable	Enables SSL key logging in the .pcapng file. It is only valid when the global <code>pcapng-enable</code> 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.

Parameter	Description
	week - Backs up the log messages generated during the most recent 7 days. days - Backs up the log messages generated using <i>days</i> 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.
<i>profile-name</i>	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 through a data interface.
<i>url</i>	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) "%&'/:<>?@[\\]

Parameter	Description
	To enter the entire URL, use one of the following: • <code>tftp://host/file</code> • <code>ftp://[user@]host[:port]/file</code> • <code>scp://[user@]host/file</code> • <code>sftp://[user@]host/file</code>
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, 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
<i>profile-name</i>	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 <code>encrypt</code> 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.
<i>url</i>	The <i>url</i> specifies the file transfer protocol, 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

Parameter	Description
	• 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, 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
<i>time</i>	Set the time, using 24-hour format hh:mm:ss.
<i>day</i>	Set the day of the month (1-31).
<i>month</i>	Set the month (January, February, March, and so on).
<i>year</i>	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
<i>filetype</i>	The following sub-options can be configured:
<code>aflex</code>	Exports an aFlex file.
<code>auth-portal</code>	Exports an authentication portal file for Application Access Management (AAM).
<code>auth-portal-image</code>	Exports the image file for the default portal.
<code>auth-saml-idp</code>	Exports the SAML metadata of the identity provider.
<code>axdebug</code> <code>[merged-pcap</code> <code> per-cpu </code> <code>tgz]</code>	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: <code>merged-pcap</code> - Export the merge file without the

Parameter	Description
	per-CPU files in PCAP format. <code>per-cpu</code> - Include the per-CPU files. <code>tgz</code> - Export the axDebug file without the per-CPU capture files in a <code>.tgz</code> format instead of PCAP format.
<code>bw-list</code>	Exports a black/white list.
<code>ca_cert</code>	Exports a CA cert file.
<code>cert</code>	Exports an SSL cert file.
<code>cert-key</code>	Exports a certificate and key together as a single file.
<code>class-list</code>	Exports an IP class list.
<code>crl</code>	Exports a certificate revocation list (CRL).
<code>csr</code>	Exports a certificate signing request.
<code>debug_monitor</code>	Exports a debug monitor file.
<code>dnssec-dns-key</code>	Exports a DNSEC key-signing key (KSK) file.
<code>dnssec-ds</code>	Exports a DNSSEC DS file.
<code>fixed-nat</code>	Exports the fixed NAT port mapping file.
<code>fixed-nat-archive</code>	Exports the fixed NAT port mapping archive file.
<code>geo-location</code>	Export the geo-location CSV file.
<code>health-external</code>	Export the external program from the system.
<code>key</code>	Exports an SSL key file.
<code>local-uri-file</code>	Exports the specified image file for the “sorry” page served to RAM Caching clients if all servers are down.
<code>lw-4o6</code>	Exports the LW-4over6 binding table file.

Parameter	Description
<code>policy</code>	Exports a WAF policy file.
<code>running-con-fig</code>	Exports the running configuration to a file.
<code>startup-con-fig profile</code>	Exports the startup configuration.
<code>store {create profile-name [options] delete profile-name}</code>	Create or delete an export store profile.
<code>syslog</code>	Exports the specified syslog file. To export syslog messages, use messages as the filename.
<code>thales-sec-world</code>	Exports a Thales security world file.
<code>visibility</code>	Export visibility module related files. <code>mon-entity-debug</code> - Export the <code>mon-entity-debug</code> file. <code>pkt-capture</code> - Export a pcapng file.
<code>tgz</code>	Export the axDebug file without the per-CPU capture files in a <code>.tgz</code> format instead of PCAP format.
<code>wsdl</code>	Exports a Web Services Definition Language (WSDL) file.
<code>xml-schema</code>	Exports an XML schema file.
<code>filename</code>	Enter the name of the file for the specified file type.
<code>use-mgmt-port</code>	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

Parameter	Description
	through a data interface. Protocol, user name (if required), and directory path you want to use to send the file.
<code>{url export- store}</code>	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: • <code>tftp://host/file</code> • <code>ftp://[user@]host[:port]/file</code> • <code>scp://[user@]host/file</code> • <code>sftp://[user@]host/file</code>

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
<i>cookie-name</i>	Name of the cookie header.
port	The port option creates a cookie based on the following format: <i>cookie-name-vportnum-groupname=encoded-ip_</i> <i>encoded-rport</i>
server	The server option creates a cookie based on the following format: <i>cookie-name=encoded-ip</i>
service-group	The service-group option creates a cookie based on the following format: <i>cookie-name-vportnum-groupname=encoded-ip_</i> <i>encoded-rport</i>

- 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
<i>ipaddr</i>	Specifies the IPv4 address of the device to test.
<i>ipv6addr</i>	Specifies the IPv6 address of the device to test.
count <i>num</i>	Specifies the number of health checks to send to the device. The default count is 1.
<i>monitor-name</i>	Specifies the name of the health monitor you want to use. The health monitor must already be configured. The default monitor is ICMP ping, which is the default Layer 3 health check.
<i>port-num</i>	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 <i>file_options1</i>	Import an aFlex file. Syntax: <pre>aflex filename {[user-tag user-tag-name] [proxy host:port] [overwrite] [use-mgmt-port] {url import-store-name terminal}</pre> Parameters: • <i>filename</i> - local file name (1-63 characters) • proxy <i>host:port</i> - 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:

Parameter	Description
	◦ An IPv6 address must be encased in a bracket, for example, <code>[a:b::1]:8080</code>. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • user-tag <i>user-tag-name</i> - 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 <i>file_options1</i>	Import a JSON web key file for Application Access Management (AAM). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
auth-portal <i>file_options1</i>	Import an authentication portal file for Application Access Management (AAM). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
auth-portal-image <i>file_options1</i>	Import an image file for the default authentication portal. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
auth-saml-idp <i>file_options2</i>	Import the SAML metadata of the identity provider. Syntax:

Parameter	Description
	auth-saml-idp <i>metadata-name</i> [verify-xml-signature] [proxy <i>host:port</i>] [overwrite] [use-mgmt-port] <i>url</i> Parameters: • <i>metadata-name</i> - Local SAML metadata name (1-63 alphanumeric characters) • verify-xml-signature - Verify metadata's XML signature • proxy <i>host:port</i> - 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 ◦ 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. • <i>url</i> - See url below.
bw-list <i>file_options1</i>	Import a black/white list. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
ca-cert <i>file_options3</i>	Imports a CA certificate without a key. ACOS distinguishes between a <i>CA cert</i> and an <i>SSL cert</i> which is imported using the syntax cert <i>file_options3</i>. CA certs are not used for handshaking with SSL clients.

Parameter	Description
	Syntax: <pre>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}</pre> Parameters: • Use the bulk option to import multiple files simultaneously as a .tgz archive. • <i>filename</i> - local file name (1-255 alphanumeric characters) • Use certificate-type {pem der pfx p7b} to specify a certificate type. • Use pfx-password <i>pswd</i> to specify the PFX certificated password if and only if you have specified the pfx certificate type. • user-tag <i>user-tag-name</i> - 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. • <i>url</i> - See url below. • <i>import-store-name</i> - Name of a file stored on ACOS drive memory. • terminal - Terminal vi operation.
cert <i>file_options3</i>	Imports an SSL certificate file. ACOS distinguishes between a <i>CA cert</i> and an <i>SSL cert</i> which is imported using the syntax ca-cert <i>file_options3</i> .

Parameter	Description
	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 <code>ca-cert file_options3</code> for information on <code>file_options3</code>.
<code>cert-key file_options4</code>	Imports a certificate and key together as a single file. Syntax: <pre>cert-key bulk [pfx-password pswd] [user-tag user-tag-name] [overwrite] [use-mgmt-port] {url import-store-name terminal}</pre> Parameters: • Use the <code>bulk</code> option to import multiple files simultaneously as a .tgz archive. • Use <code>pfx-password pswd</code> to specify the PFX certificated password if and only if the certificate type is <code>pfx</code>. • <code>user-tag user-tag-name</code> - Custom tag that can then be searched by using the aXAPI. The <code>overwrite</code> option enables the overwriting of an existing cert-key bulk file. • <code>use-mgmt-port</code> - See use-mgmt-port below. • <code>url</code> - See url below. • <code>import-store-name</code> - Name of a file stored on ACOS drive memory. • <code>terminal</code> - Terminal vi operation.

Parameter	Description
class-list <i>file_options1</i>	Import an IP class list. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .
class-list-convert <i>file_options5</i>	ACOS imports a newline delimited text file and converts it to a class-list file of the specified type: Syntax: <pre>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}</pre> Parameters: • <i>filename</i> - local file name. (1 - 63 characters) • <i>class-list-type</i> - 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 <i>SSL Insight</i> book for an example of converting to an A10 Aho-Corasick class list. • <i>string</i> - 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 <i>class-list</i> command. • user-tag <i>user-tag-name</i> - Custom tag that

Parameter	Description
	can then be searched by using the aXAPI. • proxy <i>host:port</i> - 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, <code>[a:b::1]:8080</code>. ◦ 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. • import-store-name - Name of a file stored on ACOS drive memory. • terminal - Terminal vi operation.
crl <i>file_options1</i>	Import an SSL certificate revocation list (CRL). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>. 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.

Parameter	Description
dnssec-dnskey <i>file_options1</i>	Import a DNSSEC key-signing key (KSK) file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> . The DNSSEC DNSKEY (KSK) file name can be from 1 to 127 characters.
dnssec-ds <i>file_options1</i>	Import a DNSSEC DS file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> . The DNSSEC DS file name can be from 1 to 127 characters.
file-inspection-bw-list <i>file_options1</i>	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] Parameters: use-mgmt-port - See use-mgmt-port below.
geo-location <i>file_options1</i>	Imports a geo-location data file for Global Server Load Balancing (GSLB). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .
glm-cert <i>file_options1</i>	Imports an global license manager (GLM) certificate. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .
glm-license <i>file_options1</i>	Imports an activation key license file provided by the global license manager (GLM). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .

Parameter	Description
health-external <i>file_options6</i>	Import an external health monitor program. Importing external health monitor scripts is only supported for administrative users provisioned with health monitor (<code>hm</code>) privilege. If commands with this parameter fail due to insufficient privilege, contact your ACOS root administrator. For more information, see the <i>Application Delivery and Server Load Balancing Guide (Using External Health Methods</i> section) and the <i>Management Access and Security Guide</i>. Syntax: <pre>health-external <i>program-name</i> [description <i>function</i>] [proxy <i>host:port</i>] overwrite [use-mgmt-port] <i>url</i></pre> Parameters: • <i>program-name</i> - local health monitor program name. (1 - 31 characters) • proxy <i>host:port</i> - 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, <code>[a:b::1]:8080</code> ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • overwrite - Enables the overwriting of an existing program of the same local name

Parameter	Description
	- Use the description <i>function</i> option to provide a brief description (1-63 characters) of the program purpose or function. use-mgmt-port - See use-mgmt-port below. <i>url</i> - 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 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 <i>file_options?</i>	Import the health monitor HTTP post data file. Syntax: <pre>health-postfile filename [proxy host:port] [overwrite] [use-mgmt-port] url</pre> Parameters: <i>filename</i> - local health monitor HTTP post data filename. (1 - 31 characters) proxy <i>host:port</i> - Specifies explicit HTTP proxy settings for downloading the HTTP post data

Parameter	Description
	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, <code>[a:b::1]:8080</code>. ◦ 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 <i>file_options1</i>	IP Map List file For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
key <i>file_options8</i>	Import the SSL key file. Syntax: key {bulk <i>filename</i>} [user-tag <i>user-tag-name</i>] [overwrite] [use-mgmt-port] {url import-store-name terminal} Parameters: • Use the bulk option to import multiple files simultaneously as a .tgz archive. • <i>filename</i> - local file name (1-255 alphanumeric characters) • user-tag <i>user-tag-name</i> - Custom tag that can then be searched by using the aXAPI. • The overwrite option enables the overwriting

Parameter	Description
	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 <i>file_options1</i>	Import the local URI files for HTTP responses. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
lw-4o6 <i>file_options1</i>	Import the LW-4over6 binding table file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
ng-waf-custom-page <i>html_file</i>	Import the custom HTML file for Next Generation WAF (NGWAF). Syntax: <pre>ng-waf-custom-page <i>html_file</i> { [proxy host:port] [overwrite] [use-mgmt- port]{url} }</pre> Parameters: • proxy <i>host:port</i> - 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, <i>[a:b::1]:8080</i> ◦ Only HTTP or HTTPS URLs can be specified for file downloads.

Parameter	Description
	• 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: <pre>ng-waf-module { [proxy host:port] [overwrite] [use-mgmt-port]{url} }</pre> Parameters: • proxy host:port - Specifies explicit HTTP proxy settings for downloading the NGWAF module. 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, <code>[a:b::1]:8080</code>. ◦ 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

Parameter	Description
policy <i>file_options1</i>	Import a WAF policy file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
rzp	Refer to import rpz for details.
tsig <i>file_options1</i>	Import the Trasaction Signature (TSIG) key file. The key can be private or public. Syntax: <pre>tsig filename {[user-tag user-tag-name] [overwrite] [use-mgmt-port] {url import- store-name }}</pre> Parameters: • <i>filename</i> - local file name (1-63 characters) • user-tag <i>user-tag-name</i> - 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. • <i>url</i> - See url below. • <i>import-store-name</i>- Name of a file stored on ACOS drive memory.
store <i>file_options9</i>	Import a storage name for a remote URL. • store {create <i>profile-name url</i> delete <i>profile-name</i>} • Use create to create an import store profile • Use delete to delete an import store profile • <i>profile-name</i> - name of the ACOS profile to store the remote URL (1 - 31 characters)

Parameter	Description
	<i>url</i> - See url below.
thales-secworld <i>file_options1</i>	Import a Thales security world file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
usb-license <i>file_options1</i>	Imports an activation key license file provided from a USB Key. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
web-category-license <i>file_options1</i>	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 <i>file_options1</i> syntax, see aflex <i>file_options1</i>
wsdl <i>file_options1</i>	Import a WSDL file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
xml-schema <i>file_options1</i>	Import an XML schema file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
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.
<i>url</i>	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

Parameter	Description
	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 - !#\$%()*+,-.:[]^_` ~='</li> <li>• <b>scp</b> - !#\$%()*+,-.:;[]^_`{ }~=' • http - !#\$%()*+,-.:[]^_`{ }~='</li> <li>• <b>https</b> - !#\$%()*+,-.:[]^_`{ }~=' • sftp - !#\$%()*+,-.;=^_`{ }~[] The following special characters are not supported: • tftp - No password required • scp - All are supported • ftp - -;{ } • http - #; • https - #; • sftp - %: Syntax: <pre>{ tftp://host/file ftp://[user@]host[:port]/file scp://[user@]host/file http://[user@]host/file https://[user@]host/file sftp://[user@]host/file </pre>

Parameter	Description
	} Parameters: <i>file</i> - remote file name NOTE: • This command can be executed only in the shared partition. • In case of <code>http/https</code> URL, you must replace <code>?</code> with <code>%3F</code>. For example: For <code>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 %3FlicenseKey=T3GVxx1Y</code>

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
<code>test</code>	Test the current terminal encodings for a specific

Parameter	Description
	locale.
<code>en_US.UTF-8</code>	English locale for the USA, encoding with UTF-8 (default)
<code>zh_CN.UTF-8</code>	Chinese locale for PRC, encoding with UTF-8
<code>zh_CN.GB18030</code>	Chinese locale for PRC, encoding with GB18030
<code>zh_CN.GBK</code>	Chinese locale for PRC, encoding with GBK
<code>zh_CN.GB2312</code>	Chinese locale for PRC, encoding with GB2312
<code>zh_TW.UTF-8</code>	Chinese locale for Taiwan, encoding with UTF-8
<code>zh_TW.BIG5</code>	Chinese locale for Taiwan, encoding with BIG5
<code>zh_TW.EUCTW</code>	Chinese locale for Taiwan, encoding with EUC-TW
<code>ja_JP.UTF-8</code>	Japanese locale for Japan, encoding with UTF-8
<code>ja_JP.EUC-JP</code>	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, 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 ipaddr}	Send a ping to the specified IPv4 hostname or address.
data <i>HEX-word</i>	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	Send a DS-Lite ping.

Parameter	Description
<i>ipaddr</i> [source- ipv6 <i>ipaddr</i>] <i>ipaddr</i> }	
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 <i>port-num</i> ve <i>ve-num</i> }	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 { <i>count</i> 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 <i>num</i>	Specify the size of the datagram in bytes. The default size is 84 bytes.
source { <i>ipaddr</i> ethernet <i>port-num</i> ve <i>ve-num</i> }	Forces the ACOS Device to give the specified IP address (<i>ipaddr</i>), or the IP address configured on the specified interface (either ethernet <i>port-num</i> or ve <i>ve-num</i>), as the source address of the ping.
timeout <i>secs</i>	Number of seconds the ACOS device waits for a reply to a sent ping packet.

Parameter	Description
	The default timeout value is 10 seconds.
<code>ttl num</code>	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.
<i>text</i>	Reason for the reboot.
in <i>hh:mm</i>	Schedule a reboot to take effect in the specified hours and minutes. The reboot must take place within approximately 24 hours.
at <i>hh:mm</i>	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.
<i>month</i>	Name of the month, any number of characters in a unique string.
<i>day</i>	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
<code>all</code>	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.
<code>device-id</code>	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
<i>seconds</i>	Interval at which to re-enter the command.
<i>command-options</i>	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

Parameter	Description
	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 (<i>hh:mm</i>). For example, 00:10 causes the device to shut down 10 minutes from now.
cancel	Cancel pending shutdown
<i>text</i>	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.
<i>hostname</i>	Host name of the remote system.
<i>ipaddr</i>	IP address of the remote system.
<i>login-name</i>	The user name used to log in to the remote system.
<i>protocol-port</i>	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

Parameter	Description
	through a data interface.
<i>hostname</i>	Host name of the remote system.
<i>ipaddr</i>	IP address of the remote system.
<i>protocol-port</i>	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.

Parameter	Description
	This is enabled by default.
command-timestamp	Include timestamp information in the <code>show</code> command output. The <code>unix</code> option displays the timestamp in Unix format (<code>sec.us</code>) since Unix Epoch.
editing	Enables command-line editing. This is enabled by default.
gslb-prompt <i>options</i>	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: <code>ACOS:Master(config)#</code> symbol - displays “gslb” in the CLI prompt after the name of the ACOS device. For example: <code>ACOS-gslb:Master(config)#</code>
history <i>[size]</i>	Enables and controls the command history function. The <i>size</i> option specifies the number of command lines that will be held in the history buffer. This is enabled by default.
length <i>num</i>	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.
width <i>num</i>	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.
<i>hostname</i>	Host name of the device at the remote end of the route to be traced.
<i>ipaddr</i>	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 <i>[options]</i>	Write the configuration to the configuration profile stored in the default primary configuration area.
secondary <i>[options]</i>	Write the configuration to the configuration profile stored in the default secondary configuration area.
<i>name</i> <i>[options]</i>	Write the configuration to a specified profile name.
<i>options</i>	• 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 Default profile is not linked and a custom-named profile is linked instead, please run <code>write memory</code> or <code>write memory all-partitions</code> 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.

Parameter	Description
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 <code>write memory</code> or <code>write memory all-partitions</code> 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.
<i>profile-name</i>	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.
<i>part-name</i>	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
<i>acl-num</i>	Standard ACL number (1-99).
<i>seq-num</i>	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.
13-vlan-fwd-disable	Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
remark <i>string</i>	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 <i>host-ipaddr</i>	Denies or permits traffic received from a specific, single host.
<i>src-ipaddr</i> { <i>filter-mask</i> <i>/mask-length</i> }	Denies or permits traffic received from the specified host or subnet. The <i>filter-mask</i> specifies the portion of the address to filter: • Use 0 to match. • Use 255 to ignore. For example, the <i>filter-mask</i> 0.0.0.255 filters on a 24-bit subnet. Alternatively, you can use <i>/mask-length</i> 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 <code>transparent-session-only</code> 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.

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	00001 010	00001 010	00001 010	00000 000	00000 000	11111 111	11111 111	11111 111
D	10	10	10	0	0	255	0	255
B	00001 010	00001 010	00001 010	00000 000	00000 000	11111 111	00000 000	11111 111
D	172	0	3	0	0	255	255	255
B	10101 100	00000 000	00000 010	00000 000	00000 000	11111 111	11111 111	11111 111
D	172	0	3	0	0	255	0	255
B	10101 100	00000 000	00000 010	00000 000	00000 000	11111 111	00000 000	11111 111

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 ACL to 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 it easier to introduce new access-list statements in the desired order.

Related Commands:

- [access-list \(extended\)](#)
- [disable-management](#)
- [enable-management](#)

¹This 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
<i>acl-num</i>	Extended ACL number (100-199).

Parameter	Description
<i>seq-num</i>	Sequence number of this rule in the ACL. You can use this option to re-sequence the rules in the ACL.
<i>permit</i>	Allows traffic that matches the ACL.
<i>deny</i>	Drop the traffic that matches the ACL.
<i>l3-vlan-fwd-disable</i>	Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
<i>remark string</i>	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.
<i>ip</i>	Filters on IP packets only.
<i>icmp</i>	Filters on ICMP packets only.
<i>tcp udp</i>	Filters on TCP or UDP packets, as specified. These options also allow you to filter based on protocol port numbers.
<i>object-group</i>	Object group name. Object groups provide additional flexibility in ACL management; they can simplify ACL implementations and extend the ACL number and functionality limitations.
<i>type icmp-type</i>	This option is applicable if the protocol type is <i>icmp</i>. 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"). • <i>any-type</i> – 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>code icmp-code</code>	This option is applicable if the protocol type is icmp. Matches based on the specified ICMP code. Replace <i>code-num</i> with an ICMP code number (0-254), or specify any-code to match on any ICMP code.
<code>any host host- src-ipaddr net-src- ipaddr { filter-mask /mask- length}</code>	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 <i>filter-mask</i> specifies the portion of the address to filter: ◦ Use 0 to match.

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

Parameter	Description
	Use 255 to ignore. For example, the <i>filter-mask</i> 0.0.0.255 filters on a 24-bit subnet. Alternatively, you can use <i>/mask-length</i> 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 <i>dst-port</i> gt <i>dst-port</i> lt <i>dst-port</i> range <i>start-dst-port</i> <i>end-dst-port</i>	The destination protocol ports to filter for TCP and UDP: eq <i>src-port</i> - The ACL matches on traffic from the specified destination port. gt <i>src-port</i> - The ACL matches on traffic from any destination port with a higher number than the specified port. lt <i>src-port</i> - The ACL matches on traffic from any destination port with a lower number than the specified port. range <i>start-src-port end-src-port</i> - 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 <i>vlan-id</i> [<i>ethernet</i> <i>eth-id</i> <i>trunk trunk-id</i>]	Matches on the specified VLAN. VLAN matching occurs for incoming traffic only. ethernet <i>eth-id</i> - 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 <i>trunk</i> -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 bypassed 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.
<i>cmd-level</i>	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.
<i>debug-level</i>	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
<code>active-template</code> <i>name</i>	Configures the name of the global logging template.
<code>collector-group</code> <i>name</i> {udp tcp}	Configures the name of the log servers group. Options are: • <code>udp</code> – Uses UDP syslog protocol to send messages to the log collector. • <code>tcp</code> – Uses TCP syslog protocol to send

Parameter	Description
	messages to the log collector
local-logging	• <code>enable</code> - Enables local-logging feature, by default it is disabled. • <code>rate-limit</code> - Sets the rate-limit from 1-60000, by default it is 1000. • <code>max-disk-space</code> - Sets the maximum disk space from 50-20000 MB, by default it is 100 MB. • <code>delete-old-logs-in-disk</code> - Deletes all old logs from the disk.
log-parameterization	Configures Harmony controller log parameters.
log-properties	Configures Logging related properties: • <code>add-msgid-in-header</code> - 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 <code>add-msgid-in-header</code> 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. • <code>enable-8K-tcp-syslog</code> - Enables 8K size remote TCP syslog. • <code>enable-millisec</code> - Enables the inclusion

Parameter	Description
	of milliseconds in the log timestamp. The timestamp can have a delay of up to 8 milliseconds. • NOTE: The <code>ClientTimestampFormat</code> 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. • <code>use-iso8601-timestamp</code> - 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).
<code>log-server name</code>	Name of the ACOS logging server.
<code>logdb</code>	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. • <code>enable-all</code> – Enables logging for all widgets. • <code>enable-cgn</code> – Enables CGN logging. • <code>enable-fw</code> – Enables Firewall logging. • <code>enable-http-forward-proxy</code> – Enables HTTP forward proxy logging.

Parameter	Description
	• <code>enable-smtp</code> – Enables SMTP logging. • <code>enable-ssli</code> – Enables SSLi logging. Use the <code>enable-fw</code> 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.
<code>message-id name</code>	Configures the name of the log message. The <i>name</i> should specify log message-id lineage.
<code>message-selector name</code>	Configures the message selector to select messages to be logged/blocked. Options include: • <code>rule</code> – 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: • <code>message-id name</code> – Selects a specific message by message-id and optionally severity. The following options are available: - <code>all</code> – Log messages at this level and all sub-trees - <code>node-only</code> – Log messages at this node only - <code>children-only</code> – Log messages at all sub-trees only - <code>log-field-only</code> – Log message for this Log Field only • <code>severity</code> – Selects messages with a range of severity values - alert is most severe • <code>send</code> – 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 <i>name</i> message-selector ms- <i>name</i> collector-group col- <i>name</i>	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
<i>name</i>	Name of the collector group of log servers (1-127 characters).
<i>protocol</i>	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
<i>format</i>	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: <i>SYSLOG</i>: Log message format is syslog. This is the default format. <i>CEF</i>: Log message format is cef. <i>LEEF</i>: Log message format is leef.
<i>health-check name</i>	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.
<code>log-dis- tribution</code>	Configure a log-distribution method. The options are: <i>round-robin</i>: log server selection is based on round-robin. This is the default distribution method. <i>hashing</i>: log messages at the specified node.
<code>log-server name port</code>	Configure the members (log server name and port) of the collector group.
<code>rate-limit num per seconds</code>	Apply a rate-limiter to the collector group. <i>num</i> - Maximum number of message allowed per interval (0-2147483647). <i>seconds</i> - Interval of time for <i>num</i> in seconds (1-100).
<code>sampling- enable</code>	Enable baselining.
<code>server-dis- tribution-hash</code>	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
<i>name</i>	Log server name (1-127 characters).
<i>ipv4addr</i>	Specify the IPv4 address of the remote server.
<i>ipv6addr</i>	Specify the IPv6 address of the remote server.
<i>hostname</i>	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
<code>[no] health-check</code>	Bind a configured health check to the log server. A health check can be configured using the health monitor command.
<code>[no] health-check-disable</code>	Disable any health check configured with the log server.
<code>[no] port <i>number</i> <i>protocol</i></code>	Specify a port <i>number</i> (1-65535) and <i>protocol</i> (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
<code>message-id</code> <code>lineage</code> <code>[level]</code> <code>[severity]</code>	Specify a specific message or family of messages to match by this rule. <i>lineage</i> - See acos-events message-id for a complete description about lineage. <i>level</i> - Specify one of the following: <code>all</code> - Match on all messages at the specified lineage level and all lower levels. <code>node-only</code> - Match on all messages at the specific lineage level only. <code>children-only</code> - Do not match any messages at the specified lineage level, but match all messages at all lower levels. <i>severity</i> - See <code>severity</code> below for a complete description of the severity options.

Command	Description
<code>send</code>	Send log messages that are matched by this rule.
<code>drop</code>	Drop log messages that are matched by this rule.
<code>severity</code> <code>{equal </code> <code>equal-and-</code> <code>higher}</code> <code>severity-</code> <code>level</code>	Specify a severity-level of message to match using this rule. Use <code>equal</code> to match only messages of the specified severity. Use <code>equal-and-higher</code> to match messages of the specified severity and all messages of a high severity. For example: <code>severity equal warning</code> - matches only log messages that have a level 4 (Warning) severity. <code>severity equal-and-higher warning</code> - 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
<i>admin-username</i>	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).
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 <i>level</i>	Sets the privilege <i>level</i> 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 delete these scripts are described in the <i>Command Line Reference for ADC</i>. Importing these scripts is

Command	Description
	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 confidentiality, 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 <i>Application Delivery and Server Load Balancing Guide</i> (Using <i>External Health Methods</i> section) and the <i>Management Access and Security Guide</i>. • <code>partition-read</code> – The admin has read-only privileges within the L3V partition to which the admin is assigned, and read-only privileges for the shared partition. • <code>partition-write</code> – 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. • <code>partition-enable-disable</code> – 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. • <code>partition-name</code> – The name of the L3V partition to

Command	Description
	which the admin is assigned. This option applies only to admins that have privilege level <code>partition-read</code>, <code>partition-write</code>, or <code>partition-enable-disable</code>. NOTE: L3V partitions are used in Application Delivery Partitioning (ADP). For more information, see <i>Configuring Application Delivery Partitions</i> guide. The default privilege is read.
<code>ssh-pubkey options</code>	Manage public key authentication for the admin. The <code>options</code> are as follows and described in the following rows: • <code>import</code> • <code>delete</code> • <code>list</code>
<code>ssh-pub-keyimport url</code>	Imports an authorized public key onto the ACOS device. The <code>url</code> 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: <pre>!#\$%()*+,-.:/:;<=>?@[\]^_`{ }~</pre> The following special characters are not supported: <pre>(blank space) "%&'/:;<>?@[\\</pre> To enter the entire URL:

Command	Description
	• <code>tftp://host/file</code> • <code>ftp://[user@]host[port:]/file</code> • <code>scp://[user@]host/file</code> • <code>sftp://[user@]host/file</code>
ssh-pub-key delete <i>num</i>	Deletes an authorized public key. The <i>num</i> specifies the key number on the ACOS device. The key numbers are displayed along with the keys themselves by the <code>ssh-pubkey list</code> command. This command can also be used to verify installation of the public key.
ssh-pub-key list	Lists all the authorized public keys.
trusted-host { <i>ipaddr/</i> <i>mask-</i> <i>length</i> ipaddr <i>subnet-</i> <i>mask</i> access- list <i>acl-</i> <i>id</i> }	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.

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 deny management access by admin “adminuser2” using the CLI or aXAPI:

```
ACOS(config)# admin adminuser2
ACOS(config-admin:adminuser2)# no access cli
ACOS(config-admin:adminuser2)# no 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
<i>admin-username</i>	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 } <i>options</i>	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 <i>options</i> for each cloud credentials configuration are as follows and described in the following rows: • import • delete • show
import [<i>use-mgmt-port</i>] <i>url</i>	Imports the AWS, Azure, or VMware credentials file or AWS configuration file on the ACOS device.

Command	Description
	<code>use-mgmt-port</code> - Specifies the management port as the source port. <code>url</code> - 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 characters too: <pre>!#\$()*+,-.:=^_`{ }~</pre> The following special characters are not supported: <pre>(blank space) "%&'/:;<>?@[\\]</pre> To enter the complete URL: <code>tftp://host/file</code> <code>ftp://[user@]host[port:]/file</code> <code>scp://[user@]host/file</code> <code>sftp://[user@]host/file</code>
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 <code>credentials</code> 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 <i>vThunder Installation Guides</i> .
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 <code>cloud-cred</code> 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 <code>cloud-cred</code> import file. The following files have the same location for HA and Cloud Credentials Import: • <code>/a10data/.aws/config</code> • <code>/a10data/.aws/credentials</code> • <code>/a10data/.azure/credentials</code>
Example	The following commands import the AWS credentials on an ACOS device: <pre>ACOS(config)# admin adminuser2 ACOS(config-admin:adminuser2)# cloud-cred aws-cred import tftp://192.168.0.0/credentials.txt</pre>
Example	The following command shows the imported AWS credentials file information: <pre>ACOS(config-admin:adminuser2)# cloud-cred aws-cred show [default] aws_access_key_id = XXXX aws_secret_access_key = XXXX</pre>

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 <i>minutes</i>	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.
enable	Enables the admin lockout feature. The lockout feature is disabled by default.
reset-time <i>minutes</i>	Number of minutes the ACOS device remembers failed login attempts. You can specify 1-1440 minutes. The default reset time is 10 minutes.
threshold <i>number</i>	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.

Parameter	Description
<i>session-id</i>	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 <i>src-name</i> aFlex script to <i>dst-name</i> .
create	Create an aFlex script with the specified <i>name</i> .
delete	Delete the specified aFlex script.
help	View aFlex help.
rename	Rename an aFlex script from <i>src-name</i> to <i>dst-name</i> .

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
<i>ipaddr</i>	IP address of the static entry.
<i>mac-address</i>	MAC address of the static entry.
<i>port-num</i>	Ethernet port number.
<i>trunk-id</i>	Trunk ID number.
<i>vlan-id</i>	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, 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.
<i>num-entries</i>	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
<code>ldap</code>	Use LDAP for console authentication
<code>local</code>	Use the ACOS configuration for console authentication.
<code>radius</code>	Use RADIUS for console authentication.
<code>tacplus</code>	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 <i>method1</i>. If a <i>method1</i> server replies, permit or deny access based on the server reply. • If no <i>method1</i> servers reply or a <i>method1</i> server denies access, try <i>method2</i>. • If no <i>method2</i> servers reply or a <i>method2</i> server denies access, try <i>method3</i>. • If no <i>method3</i> servers reply or a <i>method3</i> server denies access, try <i>method4</i>. 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 <i>does</i>

Parameter	Description
	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 <i>method1</i>. If a <i>method1</i> server replies, permit or deny access based on the server reply. • <i>Only</i> if no <i>method1</i> servers reply, try method2. If a <i>method2</i> server replies, permit or deny access based on the server reply • <i>Only</i> if no <i>method2</i> servers reply, try method3. If a <i>method3</i> server replies, permit or deny access based on the server reply. • <i>Only</i> if no <i>method3</i> servers reply, try <i>method4</i>. 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 option, the settings apply to all types of admin access.
type <i>method1</i> [<i>method2</i> [<i>method3</i> [<i>method4</i>]]]	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
<i>commands</i> <i>cmd-level</i> <i>method</i>	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

Parameter	Description
	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.
none	No authorization will be performed.
debug <i>debug-</i> <i>level</i>	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.

Parameter	Description
<i>feature-name</i>	The name of the feature. For example, app_fw - application firewall.
<i>check-now feature-name</i>	Manually upgrade software to the latest version (operational command).
<i>revert feature-name</i>	Manually revert software to previous successfully installed version.
<i>reset feature-name</i>	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 { <i>hh:mm</i> }	Specify the daily time to update the central-cert-pin-list. The time is <i>hh:mm</i> 24-hours local

Parameter	Description
	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 chassis platform, 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
<i>auth-type</i> { <i>ntlm</i> <i>basic</i> <i>domain</i> }	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 NTML authentication. The value can be alphanumeric and up to 127 characters are allowed.
<i>https-port</i>	Specify the proxy server HTTPS port. The value can be between 1-65535.
<i>proxy-host</i>	Specify the proxy server host name or IP address. The value can be alphanumeric and up to 127 characters are allowed.
<i>username</i>	Specify the username for proxy authentication. The value can be alphanumeric and up to 127 characters are allowed.
<i>password</i>	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 chassis platform, 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 chassis platform, 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
<code>daily{hh:mm}</code>	Specify the daily time to update the application firewall protocol bundle latest version. The time is <code>hh:mm</code> 24-hours local time format.
<code>weekly{Monday Tuesday Wednesday Thursday Friday Saturday Sunday}</code>	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.: <code>hh:mm</code>

Default Not enabled

Mode Configuration mode

Example The following example configures the automatic-update schedule:

```
ACOS(config)# automatic-update app-fw schedule daily 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 chassis platform, 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
<code>daily{hh:mm}</code>	Specify the daily time to update the CA bundle latest version. The time is <code>hh:mm</code> 24-hours local time format.
<code>weekly{Monday Tuesday Wednesday Thursday Friday Saturday Sunday}</code>	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.: <code>hh:mm</code>

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 chassis platform, 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 <i>{hh:mm}</i>	Specify the daily time to update the A10 Threat Intel list. The time is <i>hh:mm</i> 24-hours local time format.
weekly <i>{Monday Tuesday Wednesday Thursday Friday Saturday Sunday}</i>	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: <i>hh:mm</i>

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
<i>feature-name</i>	The name of the feature. For example, app_fw: application firewall.
<i>schedule weekly</i>	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.
<i>schedule daily</i>	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
<i>store-name</i>	Name of the store.
<i>url</i>	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: <pre>!#\$()*+,-.:=^_`{ }~</pre> The following special characters are not supported: <pre>(blank space) "%&'/:<>?@[\\</pre> To enter the entire URL: <pre>tftp://host/file ftp://[user@]host[port:]/file scp://[user@]host/file sftp://[user@]host/file</pre>

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
<i>target</i>	- 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.

Parameter	Description
	Specify <code>log</code> to back up the system log. You can specify either option, or both options.
hour <i>num</i> day <i>num</i> week <i>num</i>	Specifies how often to perform the back ups. You can specify one of the following: hour <i>num</i>—Performs the backup each time the specified number of hours passes. For example, specifying <code>hour 3</code> causes the backup to occur every 3 hours. You can specify 1-65534 hours. There is no default. day <i>num</i>—Performs the backup each time the specified number of days passes. For example, specifying <code>day 5</code> causes the backup to occur every 5 days. You can specify 1-199 days. There is no default. week <i>num</i>—Performs the backup each time the specified number of weeks passes. For example, specifying <code>week 4</code> 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.
<i>url</i>	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

Parameter	Description
	supports the following special characters: <pre>!#\$()*+,-.:=^_`{ }~</pre> The following special characters are not supported: <pre>(blank space) "%&'/:<>?@[\\</pre> 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, 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.
<i>line</i>	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	<code>[no] bfd echo</code>
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: ◦ <code>ip anomaly-drop drop-all</code> ◦ <code>ip anomaly-drop security-attack layer-3</code>

bfd enable

Description	Globally enable BFD packet processing.
Syntax	<code>[no] bfd enable</code>
Default	Disabled
Mode	Configuration mode

bfd interval

Description	Configure BFD timers.

Syntax

```
[no] bfd interval ms min-rx ms multiplier num
```

Parameter	Description
interval <i>ms</i>	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 <i>ms</i>	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 <i>num</i>	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	<code>block-replace-end</code>
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	<code>block-replace-start</code> 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, 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, 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)# bpd-fwd-group 1
ACOS(config-bpdu-fwd-group:1)# ethernet 1 to 3
ACOS(config-bpdu-fwd-group:1)# show bpd-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 <i>string</i>	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 <i>num</i>	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 <i>vlan-id</i> <i>... to</i> vlan <i>vlan-id</i> <i>id]</i>	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 chassis 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
<i>name</i>	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.
ipv6	For more information, see class-list (for many pools, non-LSN)
string	Create a string class-list. For more information, see class-list (string) .
string-case-insensitive	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
<i>list-name</i>	Adds the list to the running-config.
ac	Identifies this as an Aho-Corasick class list.
<i>file</i>	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
<code>[no] contains <i>sni-string</i></code>	Matches if the specified string appears anywhere within the SNI value.
<code>[no] ends-with <i>sni-string</i></code>	Matches only if the SNI value ends with the specified string.
<code>[no] equals <i>sni-string</i></code>	Matches only if the SNI value completely matches the specified string.
<code>[no] starts-with <i>sni-string</i></code>	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
<i>list-name</i>	Adds the list to the running-config.
<i>file</i>	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
<i>ipv4addr</i> [<i>/mask-length</i>] [<i>ip-limiting-</i>	Specifies the IPv4 host or subnet address of the client in standard CIDR notation. To configure a wildcard IP address, specify

Parameter	Description
<code>rule]</code>	0.0.0.0 /0. The wildcard address matches on all addresses that do not match any entry in the class list. The following <i>ip-limiting-rule</i> options are available: • <code>glid num</code> - Use the specified GLID as the IP limiting rule. • <code>lid num</code> - Use the specified LID as the IP limiting rule configured at the same level (in the same PBSLB policy template) as the class list. • <code>lsn-lid num</code> - Use the specified LSN LID as the IP limiting rule. • <code>lsn-radius-profile num</code> - 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.
<code>ipv6addr/mask-length [ip-limiting-rule]</code>	Specifies the IPv6 host and subnet address of the client in standard CIDR notation. The available <i>ip-limiting-rules</i> are the same as the <i>ipv4addr</i> 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
<i>list-name</i>	Adds the list to the running-config.
<i>dns</i>	Identifies this list as a DNS class list.
<i>file</i>	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
<i>match-option</i>	Specifies the match criteria for the <i>domain-string</i> . The <i>match-option</i> can be one of the following: <code>dns contains</code> – The entry matches if the DNS request is for a domain name that contains the <i>domain-string</i> anywhere within the requested domain name. <code>dns starts-with</code> – The entry matches if the DNS request is for a domain name that begins with the <i>domain-string</i> . <code>dns ends-with</code> – The entry matches if the DNS request is for a domain name that ends with the <i>domain-string</i> .

Parameter	Description
<i>domain-string</i>	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 <code>dns contains</code>, <code>dns starts-with</code>, and <code>dns ends-with</code> options. For example, “dns ends-with example.com” matches on both abc.example.com and www.example.com.
<i>glid num</i> <i>lid num</i>	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 <code>glid num</code> option. The <code>lid num</code> 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 <i>domain-string</i>. 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 <i>Command Line Interface Reference for ADC</i> .

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
<i>list-name</i>	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
<i>ipaddr</i> <i>/network-mask</i>	Specifies the IPv4 host or subnet address of the client. The <i>network-mask</i> 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.
<i>ipv6-addr /subnet-length</i>	Specifies the IPv6 host or network address of the client.
<i>ip-limiting-rule</i>	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. • <i>glid num</i> - Use the specified GLID as the IP limiting rule. • <i>lid num</i> - Use the specified LID as the IP limiting rule configured at the same level (in the same PBSLB policy template) as the class list. • <i>lsn-lid num</i> - Use the specified LSN LID as the IP limiting rule. • <i>lsn-radius-profile num</i> - 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 <i>pool-name</i> 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
<code>list-name</code>	Adds the list to the running-config.
<code>file</code>	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.
<code>string</code>	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
<code>list-name</code>	Adds the list to the running-config.
<code>file</code>	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.
<code>string-case-insensitive</code>	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 <i>name</i>	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 <i>name</i>	Authenticate using the specified private key.
<i>dest-ipaddress</i>	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
<code>use-mgmt-port</code>	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.
<code>url</code>	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: • <code>tftp://host/file</code> • <code>ftp://[user@]host[port:]/file</code> • <code>scp://[user@]host/file</code> • <code>sftp://[user@]host/file</code>
<code>from-profile-name</code>	Configuration profile you are copying from.
<code>to-profile-name</code>	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
<i>file-type</i>	Type of file to be deleted: • <code>auth-portal</code> (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)
<i>file-name</i>	Name of the file you want to delete.

Parameter	Description
	NOTE: • For the <code>geo-location</code> option, you can specify <code>all</code> instead of a specific <code>file-name</code> to delete all files. • There is no file-name option for <code>web-category database</code>.

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
<i>server-name</i>	Disables the specified real or virtual server.
port <i>port-num</i>	Disables only the specified service port. If you omit the <i>server-name</i> 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 10](#) lists the default settings for each management service.

Table 10 : 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 `a11` 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, 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	<code>[no] standalone</code>
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
<code>[no] algorithm</code> <code>{RSASHA1 </code> <code>RSASHA256 </code> <code>RSASHA512}</code>	Cryptographic algorithm to use for encrypting DNSSEC keys. The default algorithm is RSASHA256.
<code>[no]</code> <code>combinations-</code> <code>limit <i>num</i></code>	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
<code>[no] dnskey-ttl seconds</code>	Lifetime for DNSSEC key resource records. The TTL can range from 1-864,000 seconds. The default is 14,400 seconds (4 hours).
<code>[no] enable-nsec3</code>	Enables NSEC3 support. This is disabled by default.
<code>[no] hsm template-name</code>	Binds a Hardware Security Module (HSM) template to this DNSSEC template.
<code>[no] ksk keysize bits</code>	Key length for KSKs. You can specify 1024-4096 bits. The default is 2048 bits.
<code>[no] ksk lifetime seconds</code> <code>[rollover-time seconds]</code>	Lifetime for KSKs, 1-2147483647 seconds (about 68 years). The <code>rollover-time</code> specifies how long to wait before generating a standby key to replace the current key. The <code>rollover-time</code> setting also can be 1-2147483647 seconds. Generally, the <code>rollover-time</code> 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 <code>rollover-time</code> 30931200 seconds (358 days)
<code>[no] return-nsec-on-failure</code>	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.
<code>[no] signature-validity-period days</code>	Period for which a signature will remain valid. The time can range from 5 to 30 days. The default is 10 days.

Command	Description
<code>[no] zsk lifetime seconds [rollover-time seconds]</code>	Lifetime for ZSKs, 1-2147483647 seconds. The <code>rollover-time</code> specifies how long to wait before generating a standby key to replace the current key. The <code>rollover-time</code> setting also can be 1-2147483647 seconds. Generally, the <code>rollover-time</code> 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 <code>rollover-time</code> 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
<i>zone-name</i>	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	<code>do command</code>
Default	N/A
Mode	Configuration mode
Example	The following command runs the <code>traceroute</code> 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
<code>domain-name</code>	Specify a domain name (1-127 characters) to be added to the domain list.
<code>interval</code> <code><minutes></code>	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.
<code>fail-interval</code> <code><seconds></code>	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
<code>acl-v4</code> <i>id</i>	Permits or denies management access based on permit or deny rules in the ACL for IPv4 addresses.
<code>acl-v6</code> <i>id</i>	Permits or denies management access based on permit or deny rules in the ACL for IPv6 addresses.
<code>http</code>	Allows HTTP access to the management GUI.
<code>https</code>	Allows HTTPS access to the management GUI.
<code>ntp</code>	Controls access to the NTP server on ACOS.
<code>ping</code>	Allows ping replies from ACOS interfaces. This option does not affect the ACOS device's ability to ping other devices.
<code>snmp</code>	Allows SNMP access to the ACOS device's SNMP agent.
<code>ssh</code>	Allows SSH access to the CLI.
<code>telnet</code>	Allows Telnet access to the CLI.

NOTE: The management interface supports only a single ACL.

NOTE: IPv6 ACLs are supported for management access through Ethernet data interfaces and the management interface.

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 enable access, using the following options:

- `ethernet portnum [to portnum]`

Enable access for the specified protocol on the specified Ethernet interface. Use the `[to portnum]` option to specify a range of Ethernet interfaces.

- `management`

Enable access for the specified protocol on the management interface.

- **ve ve-num [to ve-num]**

Enable 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 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, use the **device-context** command to specify the device in the chassis to which this command must apply.

IPv6 ACLs are supported for management access through Ethernet data interfaces and the management interface.

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.

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, see [Adding 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 <i>num</i>	Low temperature threshold in Celcius; a log is generated when the temperature drop below this threshold.
medium <i>num</i>	Medium temperature threshold in Celcius. This threshold causes the status in the show environment command to change between "low/med" or "med/high".
high <i>num</i>	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 degrees 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
<i>num</i>	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
```

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.

Parameter	Description
	The <code>preserve-management</code> 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.
<code>preserve-accounts</code>	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.
<code>reload</code>	Reloads ACOS after the configuration erasure is completed. NOTE: When performing <code>erase preserve-management reload</code>, 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
<code>part-create</code>	Generate an event when a partition is created.
<code>part-del</code>	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-timeout <i>seconds</i>	Number of seconds fail-safe detects the dataplane hung before the ACOS device reboots. You can specify 1-30 seconds.
fpga-buff-recovery-threshold <i>256-buffer-units</i>	Minimum required number of free (available) FPGA 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).
hw-error-monitor-disable	Disables fail-safe monitoring and recovery for hardware errors. This is enabled by default.
hw-error-	Enables fail-safe monitoring and recovery for

Parameter	Description
<code>monitor-enable</code>	hardware errors. This is enabled by default.
<code>hw-error-recovery-timeout</code> <i>minutes</i>	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).
<code>session-memory-recovery-threshold</code> <i>percentage</i>	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: <u>fail-safe sw-error-monitor-enable</u> must be configured to trigger the session memory recovery threshold.
<code>sw-error-monitor-enable</code>	Enables fail-safe monitoring and recovery for software errors. This is disabled by default.
<code>sw-error-recovery-timeout</code> <i>minutes</i>	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 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.

Parameter	Description
<code>total-memory-size-check</code> <i>Gb</i> { <code>kill</code> <code>log</code> }	Amount of memory the device must have after booting. • <i>Gb</i> - Minimum amount of memory required. • <code>kill</code> – Stops data traffic and generates a message. However, the management port remains accessible. • <code>log</code> – 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.

Parameter	Description
	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 <i>file_name</i>	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
<code>[no] conn-limit num</code>	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.
<code>[no] conn-rate-limit num per num-of-100ms</code>	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.
<code>[no] dns options</code>	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 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.

Command	Description
<pre>[no] dns64 options</pre>	Configure settings for IPv6 DNS features. The following options are available: • disable • exclusive-answer • IPv6 prefix For details, see glid (for NAT64 override).
<pre>[no] over- limit- action [forward reset] [lockout minutes] [log minutes]</pre>	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 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.

Command	Description
	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 <i>num</i>	Specifies the maximum number of concurrent Layer 7 requests allowed for a client. You can specify 1-1048575.
[no] request-rate-limit <i>num per num-of-100ms</i>	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 <i>pool-name</i>	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
<code>[no] check-rate threshold</code>	Change the health-check rate limiting threshold. Replace <i>threshold</i> 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.
<code>[no] disable-auto-adjust</code>	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 processing. Auto-adjust mode is enabled by default.

Command	Description
[no] external-rate <i>scripts</i> per <i>100-ms-units</i>	Specify the maximum number of external health-checks scripts the ACOS device is allowed to perform during a given interval. <i>scripts</i> – Maximum number of scripts. <i>100-ms-units</i> – Interval to which <i>scripts</i> option applies.
interval <i>i-sec</i> [timeout <i>t-sec</i>]	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>i-sec</i> – period between health check attempts (seconds). <i>t-sec</i> – period ACOS waits for a reply to a health check (seconds). This value must be less than or equal to <i>i-sec</i>. NOTE: The timeout parameter is not applicable to external health monitors.
multi-process <i>num</i>	Enable multiple CPUs for health monitoring processes. The default setting is 1 CPU. Replace <i>num</i> 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 <i>number</i>	Maximum number of times ACOS will send the same health check to an unresponsive server before determining that the server is down.
up-retry <i>number</i>	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, <code>no up-retry 10</code>. 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: <pre>ACOS(config)# health global ACOS(config-health:global)# retry 5</pre>
Example	This command globally changes the interval and timeout to 10 seconds. <pre>ACOS(config-health:global)# interval 10 timeout 10</pre>

health monitor

Description	Configure a health monitor.
Syntax	<pre>[no] health monitor <i>monitor-name</i></pre> This command changes the CLI to the configuration level for the health monitor. See <i>Related Commands</i> 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 <i><pool-name></i>	Specifies the name of the source NAT pool for IPv4 traffic.
source-nat-pool-v6 <i><pool-name-v6></i>	Specifies the name of the source NAT pool for IPv6 traffic.
smart-nat-precedence	Configures ACOS using smart NAT

Parameter	Description
[vrid<vrid-value>]	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 <i><ethernet ve trunk><intf-num></i>	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 Configuration 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
<i>ipaddr</i>	IPv4 or IPv6 address of the device you want to test.
count <i>num</i>	Wait for count tests (1-65535). The default count is 1.
monitorname <i>name</i>	Specify the pre-configured health monitor to use for the test.
port <i>portnum</i>	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), hyphen (-), 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, use the `device-context` command to specify the device in the 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.
[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).

Command	Description
[no] <code>sec-world</code>	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
<code>normal-rate</code>	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.
<code>lockup max-rate</code>	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

Parameter	Description
	larger than the normal rate.
<i>lockup-time</i>	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
<i>normal-</i>	Maximum number of ICMPv6 packets allowed per

Parameter	Description
<i>rate</i>	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 <i>max-rate</i>	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.
<i>lockup-time</i>	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 <i>filename_</i> <i>options1</i>	Import an aFlex file. Syntax: <pre>aflex <i>filename</i> {[user-tag <i>user-tag-name</i>] [proxy <i>host:port</i>] [overwrite] [use-mgmt- port] {<i>url</i> <i>import-store-name</i> terminal}</pre> Parameters: • <i>filename</i> - local file name (1-63 characters) • proxy <i>host:port</i> - 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, <i>[a:b::1]:8080</i>. ◦ Only HTTP or HTTPS URLs can be specified for file downloads. • user-tag <i>user-tag-name</i> - 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. • <i>url</i> - See url below. • <i>import-store-name</i> - Name of a file stored on ACOS drive memory. • terminal - Terminal vi operation.
auth-jwks <i>filename_</i> <i>options1</i>	Import a JSON web key file for Application Access Management (AAM).

Parameter	Description
	For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .
auth-portal <i>file_options1</i>	Import an authentication portal file for Application Access Management (AAM). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .
auth-portal-image <i>file_options1</i>	Import an image file for the default authentication portal. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i> .
auth-saml-idp <i>file_options2</i>	Import the SAML metadata of the identity provider. Syntax: auth-saml-idp <i>metadata-name</i> [verify-xml-signature] [proxy <i>host:port</i>] [overwrite] [use-mgmt-port] <i>url</i> Parameters: • <i>metadata-name</i> - Local SAML metadata name (1-63 alphanumeric characters) • verify-xml-signature - Verify metadata's XML signature • proxy <i>host:port</i> - 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 <i>file_options1</i>	Import a black/white list. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
ca-cert <i>file_options3</i>	Imports a CA certificate without a key. ACOS distinguishes between a <i>CA cert</i> and an <i>SSL cert</i> which is imported using the syntax cert <i>file_options3</i>. CA certs are not used for handshaking with SSL clients. Syntax: <pre>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}</pre> Parameters: - Use the bulk option to import multiple files simultaneously as a .tgz archive. <i>filename</i> - local file name (1-255 alphanumeric characters) - Use certificate-type {pem der pfx p7b} to specify a certificate type. - Use pfx-password <i>pswd</i> to specify the PFX certificated password if and only if you have specified the pfx certificate type.

Parameter	Description
	• user-tag <i>user-tag-name</i> - 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 <i>file_options3</i>	Imports an SSL certificate file. ACOS distinguishes between a <i>CA cert</i> and an <i>SSL cert</i> which is imported using the syntax ca-cert <i>file_options3</i>. 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 <i>file_options3</i> for information on <i>file_options3</i>.
cert-key <i>file_options4</i>	Imports a certificate and key together as a single file. Syntax: <pre>cert-key bulk [pfx-password <i>pswd</i>] [user-tag <i>user-tag-name</i>] [overwrite] [use-mgmt-port] {<i>url</i> <i>import-store-name</i> terminal}</pre> Parameters:

Parameter	Description
	• Use the bulk option to import multiple files simultaneously as a .tgz archive. • Use pfx-password <i>pswd</i> to specify the PFX certificated password if and only if the certificate type is pfx. • user-tag <i>user-tag-name</i> - 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. • <i>url</i> - See url below. • <i>import-store-name</i> - Name of a file stored on ACOS drive memory. • terminal - Terminal vi operation.
class-list <i>file_options1</i>	Import an IP class list. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
class-list-convert <i>file_options5</i>	ACOS imports a newline delimited text file and converts it to a class-list file of the specified type: Syntax: <pre>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}</pre> Parameters: • <i>filename</i> - local file name. (1 - 63 characters)

Parameter	Description
	<code>class-list-type</code> - type of class list: <code>ac</code> - Aho-Corasick class list. See the “How to Convert Your SNI List to an A10 Class List” section in the <i>SSL Insight</i> book for an example of converting to an A10 Aho-Corasick class list. <code>string</code> - string class list <code>ipv4</code> - ipv4 class list <code>ipv6</code> - ipv6 class list <code>string-case-insensitive</code> - string case insensitive class list NOTE: Only the Aho-Corasick class list is compliant with the class list types created through the <code>class-list</code> command. <code>user-tag user-tag-name</code> - Custom tag that can then be searched by using the aXAPI. <code>proxy host:port</code> - 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, <code>[a:b::1]:8080</code>. - Only HTTP or HTTPS URLs can be specified for file downloads. <code>overwrite</code> - Enables the overwriting of an existing file of the same local name. <code>use-mgmt-port</code> - See use-mgmt-port below. <code>url</code> - See url below.

Parameter	Description
	<i>import-store-name</i> - Name of a file stored on ACOS drive memory. terminal - Terminal vi operation.
crl <i>file_options1</i>	Import an SSL certificate revocation list (CRL). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>. 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 <i>file_options1</i>	Import a DNSSEC key-signing key (KSK) file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>. The DNSSEC DNSKEY (KSK) file name can be from 1 to 127 characters.
dnssec-ds <i>file_options1</i>	Import a DNSSEC DS file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>. The DNSSEC DS file name can be from 1 to 127 characters.
file-inspection-bw-list <i>file_options1</i>	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 <i>file_options1</i>	Imports a geo-location data file for Global Server Load Balancing (GSLB). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
glm-cert <i>file_options1</i>	Imports an global license manager (GLM) certificate. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
glm-license <i>file_options1</i>	Imports an activation key license file provided by the global license manager (GLM). For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>.
health-external <i>file_options6</i>	Import an external health monitor program. Importing external health monitor scripts is only supported for administrative users provisioned with health monitor (<i>hm</i>) privilege. If commands with this parameter fail due to insufficient privilege, contact your ACOS root administrator. For more information, see the <i>Application Delivery and Server Load Balancing Guide (Using External Health Methods</i> section) and the <i>Management Access and Security Guide</i>. Syntax: health-external <i>program-name</i> [description <i>function</i>] [<i>proxy host:port</i>] overwrite [<i>use-mgmt-port</i>] <i>url</i> Parameters:

Parameter	Description
	• <i>program-name</i> - local health monitor program name. (1 - 31 characters) • proxy <i>host:port</i> - 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 <i>function</i> option to provide a brief description (1-63 characters) of the program purpose or function. • use-mgmt-port - See use-mgmt-port below. <i>url</i> - 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 <i>file_options7</i>	Import the health monitor HTTP post data file. Syntax: <pre>health-postfile filename [proxy host:port] [overwrite] [use-mgmt-port] url</pre> Parameters: • <i>filename</i> - local health monitor HTTP post data filename. (1 - 31 characters) • proxy <i>host:port</i> - 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, <i>[a:b::1]:8080</i>. ◦ 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. • <i>url</i> - See url below.
ip-map-list <i>file_options1</i>	IP Map List file For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>

Parameter	Description
key <i>file_options8</i>	Import the SSL key file. Syntax: <pre>key {bulk <i>filename</i>} [user-tag <i>user-tag-name</i>] [overwrite] [use-mgmt-port] {<i>url</i> <i>import-store-name</i> terminal}</pre> Parameters: • Use the bulk option to import multiple files simultaneously as a .tgz archive. • <i>filename</i> - local file name (1-255 alphanumeric characters) • user-tag <i>user-tag-name</i> - 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. • <i>url</i> - See url below. • <i>import-store-name</i> - Name of a file stored on ACOS drive memory. • terminal - Terminal vi operation.
local-uri-file <i>file_options1</i>	Import the local URI files for HTTP responses. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
lw-4o6 <i>file_options1</i>	Import the LW-4over6 binding table file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
ng-waf-custom-page <i>html_file</i>	Import the custom HTML file for Next Generation WAF (NGWAF). Syntax:

Parameter	Description
	ng-waf-custom-page <i>html_file</i> {[proxy <i>host:port</i>] [overwrite] [use-mgmt-port]{<i>url</i>} } Parameters: • proxy <i>host:port</i> - 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, <i>[a:b::1]:8080</i> ◦ 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. • <i>url</i> - See url below. NOTE: The HTML file size should not exceed 100 KB.
ng-waf-module	Import the Next Generation WAF (NGWAF) module. Syntax: <pre>ng-waf-module {[proxy <i>host:port</i>] [overwrite] [use-mgmt-port]{<i>url</i>} }</pre> Parameters: • proxy <i>host:port</i> - 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, <code>[a:b::1]:8080</code>. ◦ 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
policy <i>file_options1</i>	Import a WAF policy file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
rzp	Refer to import rpz for details.
tsig <i>file_options1</i>	Import the Trasaction Signature (TSIG) key file. The key can be private or public. Syntax: <pre>tsig filename {[user-tag user-tag-name] [overwrite] [use-mgmt-port] {url import-store-name }}</pre> Parameters: • <i>filename</i> - local file name (1-63 characters) • user-tag <i>user-tag-name</i> - Custom tag that can then be searched by using the aXAPI.

Parameter	Description
	- The overwrite option enables overwriting the 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.
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 <i>file_options1</i> syntax, see aflex file_options1
usb-license file_options1	Imports an activation key license file provided from a USB Key. For the <i>file_options1</i> 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 <i>file_options1</i> syntax, see aflex file_options1
wsdl file_options1	Import a WSDL file. For the <i>file_options1</i> syntax, see aflex file_options1

Parameter	Description
	<i>options1</i>
xml-schema <i>file_options1</i>	Import an XML schema file. For the <i>file_options1</i> syntax, see aflex <i>file_options1</i>
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.
<i>url</i>	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 - !#\$%()*+,-.:[]^_` ~=  </li> <li>• <b>scp</b> - !#\$%()*+,-.:;[]^_`{ }~= • http - !#\$%()*+,-.:[]^_`{ }~=  </li> <li>• <b>https</b> - !#\$%()*+,-.:[]^_`{ }~= • sftp - !#\$%()*+,-.;=^_`{ }~[] The following special characters are not supported: • tftp - No password required

Parameter	Description
	• scp - All are supported • ftp - -; {} • http - #; • https - #; • sftp - %: Syntax: <pre>{ tftp://host/file ftp://[user@]host[:port]/file scp://[user@]host/file http://[user@]host/file https://[user@]host/file sftp://[user@]host/file }</pre> Parameters: <i>file</i> - remote file name

Parameter	Description
	NOTE: • This command can be executed only in the shared partition. • In case of <code>http/https</code> URL, you must replace <code>?</code> with <code>%3F</code>. For example: For <code>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 %3FlicenseKey=T3GVxx1Y</code>

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 chassis platform, 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.

Description

Syntax `import-periodic file-type options`

Parameter	Description
aflex <i>file</i> <i>options1</i>	Imports an aFlex file.

Parameter	Description
<code>auth-jwks</code> file options1	Imports a JSON web key file for Application Access Management (AAM).
<code>auth-portal</code> file options1	Imports an authentication portal file for Application Access Management (AAM).
<code>bw-list</code> file options1	Imports a black/white list.
<code>class-list</code> file options1	Imports an IP class list.
<code>class-list-convert</code> file options3	ACOS imports a newline delimited text file and converts it to a class-list file of the type specified by <code>class-list-type</code> .
<code>dnssec-dnskey</code> file options1	Imports a DNSSEC key-signing key (KSK) file.
<code>dnssec-ds</code> file options1	Imports a DNSSEC DS file.
<code>file-inspection-bw-list</code> file options2	Imports a Cylance black and white list from Cylance.
<code>geo-location</code> file options1	Imports a geo-location data file for Global Server Load Balancing (GSLB).
<code>glm-license</code> file options1	Imports an activation key license file provided by the global license manager (GLM).
<code>ip-map-list</code> file options1	IP Map List file
<code>local-uri-file</code> file options1	Imports a local URI file.
<code>policy</code> file options1	Imports a WAF policy file.
<code>rpz</code> file options1	Imports an Response Policy Zone (rpz) file.
<code>ssl-cert</code> file options4	Imports an SSL certificate.

Parameter	Description
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
<i>file_options1</i>	Syntax: <pre>filename [use-mgmt-port] url period seconds</pre> Syntax Parameters • <i>filename</i> - local file name. • use-mgmt-port • url • period seconds
<i>file_options2</i>	Syntax: <pre>[use-mgmt-port] url period seconds</pre> Syntax Parameters • use-mgmt-port • period seconds

Parameter Option	Parameter Option Description and Syntax
<i>file_</i> <i>options3</i>	Syntax: <pre>class-list-convert <i>filename</i> class-list-type {ac string ipv4 ipv6 string-case-intensive} [use-mgmt-port] <i>url</i> period <i>seconds</i></pre> Syntax Parameters: • <i>filename</i> - 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 <i>SSL Insight</i> 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 <code>class-list</code> command. • use-mgmt-port • url • period seconds
<i>file_</i> <i>options4</i>	Syntax: <pre>ssl-cert {bulk <i>filename</i>} [certificate-type {pem der pfx p7b}] [<i>pswd</i>] [use-mgmt-port] <i>url</i> period <i>seconds</i></pre>

Parameter Option	Parameter Option Description and Syntax
	Syntax Parameters: • Use the bulk option to import multiple files simultaneously as a .tgz archive. • <i>filename</i> - local file name. • Use certificate-type {pem der pfx p7b} to specify a certificate type. • Use <i>pswd</i> to specify the PFX certificated password if you have specified the pfx certificate type. • use-mgmt-port • url • period seconds
<i>file_options5</i>	Syntax: <pre>ssl-cert-key bulk [use-mgmt-port] url period seconds</pre> Syntax Parameters: The bulk keyword imports a .tgz archive. • use-mgmt-port • url • period seconds
<i>file_options6</i>	Syntax: <pre>ssl-crl filename [use-mgmt-port] url period seconds</pre> Syntax Parameters: • <i>filename</i> - local file name. • use-mgmt-port

Parameter Option	Parameter Option Description and Syntax
	• url • period seconds
<i>file_options7</i>	Syntax: <pre>ssl-key {bulk filename} [use-mgmt-port] url period seconds</pre> Syntax Parameters: The bulk keyword imports a .tgz archive containing the ssl-key file. • <i>filename</i> - local file name. • use-mgmt-port • url • period seconds
<i>file_options8</i>	Syntax: <pre>thales-kmdata filename [overwrite] [use-mgmt-port] url period seconds</pre> Syntax Parameters: • <i>filename</i> - local file name. The overwrite option enables the overwriting of existing Thales KMdata files of the same local name • use-mgmt-port • url • period seconds
<i>url</i>	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

Parameter Option	Parameter Option Description and Syntax
	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 - !#\$%()*+,-.:[]^_`{ }~</li> <li>• <b>scp</b> - !#\$%()*+,-.:[]^_`{ }~ • http - !#\$%()*+,-.:[]^_`{ }~</li> <li>• <b>https</b> - !#\$%()*+,-.:[]^_`{ }~ • sftp - !#\$%()*+,-.:[]^_`{ }~ The following special characters are not supported: • tftp - No password required • scp - All are supported • ftp - -;{ } • http - #; • https - #; • sftp - %: Syntax: <pre> { tftp://host/file ftp://[user@]host[:port]/file scp://[user@]host/file http://[user@]host/file https://[user@]host/file sftp://[user@]host/file </pre>

Parameter Option	Parameter Option Description and Syntax
	} Syntax Parameters: <i>file</i> - remote file name
period <i>seconds</i>	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. 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-	Uses the management interface as the source interface

Parameter Option	Parameter Option Description and Syntax
port	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
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)

Parameter	Description
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
<i>rpz_name</i>	Enter the file name (1-63 characters).
overwrite	Specify this option to overwrite the existing RPZ file of the same local name.
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.

Parameter	Description
user-tag <i>user-tag-name</i>	Specify this option along with the custom tag that can be searched using the aXAPI.
zone-transfer { overwrite use-mgmt-port user-tag <i>user-tag-name</i> axfr: <i>file</i> <i>import-store-name</i> }	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-tag user-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: <i>//[tsig-keyfile@]host/domain-name)</i> NOTE: The TSIG public key, as well as private key, must be present on the system while importing an RPZ file using AXFR protocol.
<i>url</i>	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 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: { <i>tftp://host/file</i>

Parameter	Description
	<pre> ftp://[user@]host[:port]/file</pre> <pre> scp://[user@]host/file</pre> <pre> http://[user@]host/file</pre> <pre> https://[user@]host/file</pre> <pre> sftp://[user@]host/file }</pre> NOTE: This command can be executed only in the shared partition.
<i>import-store-name</i>	Specify the name of a file stored on the ACOS drive memory.

Mode Privileged EXEC mode or global configuration mode

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 <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.
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 `13-vlan-fwd-disable` action.

The [show slb switch](#) is used to display statistics for this option.

Related Commands:

- [13-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
<i>fwd-port</i>	Peer member that will forward LACP packets.
<i>rcv-port</i>	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}
{cn cn-name | dn dn-name |
  domain domain-name [base base-domain] [group group-id] }
[port portnum]
[ssl]
[timeout seconds]
```

Parameter	Description
<i>hostname</i>	Host name of the LDAP server.
<i>ipaddr</i>	IP address of the LDAP Server.
<i>cn-name</i>	Value for the Common Name (CN) attribute.
<i>dn-name</i>	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=maxcra,dc=com The following string <i>is not</i> valid because of the quotation marks and space character: "cn=xxx3,dc=max cra,dc=com"
<i>domain-name</i>	Active Directory domain name.
<i>base-domain</i>	Base domain to which the user belongs.
<i>group-id</i>	Group ID to which the user belongs.
<i>portnum</i>	Protocol port on which the server listens for LDAP traffic. The default is 389.

Parameter	Description
<i>seconds</i>	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.
<i>ssl</i>	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                                         |
|----------------|-----------------------------------------------------|
| <b>default</b> | Links “startup-config” to the configuration profile |

| Parameter                         | Description                                                                                      |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
|                                   | stored in the image area from which the ACOS device was most recently rebooted.                  |
| <i>profile-name</i>               | Links “startup-config” to the specified configuration profile.                                   |
| <b>primary</b>   <b>secondary</b> | 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).

|                |                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <pre>[no] lldp management-address       {dns dns-value   ipv4 ipv4-value ipv6 ipv6-value}       interface {ethernet eth-num   management   ve ve-num}</pre> |
| <b>Default</b> | Not set                                                                                                                                                     |
| <b>Mode</b>    | Configuration mode                                                                                                                                          |
| <b>Usage</b>   | LLDP commands are only available in the shared partition.                                                                                                   |

## lldp notification interval

|                    |                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This object controls the interval between transmission of LLDP notifications during normal transmission periods. |
| <b>Syntax</b>      | <pre>[no] lldp notification interval notification-value</pre>                                                    |
| <b>Default</b>     | 30                                                                                                               |
| <b>Mode</b>        | Configuration mode                                                                                               |
| <b>Usage</b>       | LLDP commands are only available in the shared partition.                                                        |

## lldp system-description

|                    |                                                                            |
|--------------------|----------------------------------------------------------------------------|
| <b>Description</b> | Defines the alpha-numeric string that describes the system in the network. |
| <b>Syntax</b>      | <pre>[no] lldp system-description sys-description-value</pre>              |
| <b>Default</b>     | None                                                                       |
| <b>Mode</b>        | Configuration mode                                                         |
| <b>Usage</b>       | LLDP commands are only available in the shared partition.                  |

## lldp system-name

|                    |                                                              |
|--------------------|--------------------------------------------------------------|
| <b>Description</b> | Defines the string that will be assigned as the system name. |
| <b>Syntax</b>      | <pre>[no] lldp system-name system-name-value</pre>           |

|                |                                                                      |
|----------------|----------------------------------------------------------------------|
| <b>Default</b> | hostname                                                             |
| <b>Mode</b>    | Configuration mode                                                   |
| <b>Usage</b>   | LLDP commands are only available in the shared partition.            |
| <b>Example</b> | The following command will set the LLDP system name to “testsystem”: |

```
ACOS(config)# lldp system-name testsystem
```

## lldp tx fast-count

|                    |                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | 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. |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|               |                                                          |
|---------------|----------------------------------------------------------|
| <b>Syntax</b> | <code>[no] <b>lldp tx fast-count</b> <i>value</i></code> |
|---------------|----------------------------------------------------------|

|                |   |
|----------------|---|
| <b>Default</b> | 4 |
|----------------|---|

|             |                    |
|-------------|--------------------|
| <b>Mode</b> | Configuration mode |
|-------------|--------------------|

|              |                                                           |
|--------------|-----------------------------------------------------------|
| <b>Usage</b> | LLDP commands are only available in the shared partition. |
|--------------|-----------------------------------------------------------|

|                |                                                                                     |
|----------------|-------------------------------------------------------------------------------------|
| <b>Example</b> | 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

|                    |                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | 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. |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|               |                                                |
|---------------|------------------------------------------------|
| <b>Syntax</b> | <code>[no] <b>lldp tx fast-interval</b></code> |
|---------------|------------------------------------------------|

|                |          |
|----------------|----------|
| <b>Default</b> | 1 second |
|----------------|----------|

|             |                    |
|-------------|--------------------|
| <b>Mode</b> | Configuration mode |
|-------------|--------------------|

|              |                                                           |
|--------------|-----------------------------------------------------------|
| <b>Usage</b> | 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

|                    |                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | Indicates the delay interval when the administrative status indicates 'disabled' after which re-initialization is attempted. The range for the <i>reinit-delay-value</i> is 1-5 seconds. |
| <b>Syntax</b>      | <code>[no] lldp tx reinit-delay reinit-delay-value</code>                                                                                                                                |
| <b>Default</b>     | 2 seconds                                                                                                                                                                                |
| <b>Mode</b>        | Configuration mode                                                                                                                                                                       |
| <b>Usage</b>       | LLDP commands are only available in the shared partition.                                                                                                                                |
| <b>Example</b>     | The following command will set the retransmission delay to 3 seconds:<br><br><code>ACOS(config)# lldp tx reinit-delay 3</code>                                                           |

## locale

|                    |                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | Set the CLI locale.                                                                                                                                                                                                                                           |
| <b>Syntax</b>      | <code>[no] locale {test   locale}</code>                                                                                                                                                                                                                      |
| <b>Default</b>     | en_US.UTF-8                                                                                                                                                                                                                                                   |
| <b>Mode</b>        | Configuration mode                                                                                                                                                                                                                                            |
| <b>Usage</b>       | Use this command to configure the locale or to test the supported locales.<br><br>If the ACOS device is a member of an aVCS virtual chassis, use the <code>device-context</code> command to specify the device in the chassis to which to apply this command. |
| <b>Example</b>     | The following commands test the Chinese locales and set the locale to zh_CN.GB2312:<br><br><code>ACOS(config)# locale test zh_CN</code><br><code>ACOS(config)# locale zh_CN.GB2312</code>                                                                     |

## 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                                                                                                                                                                                                                                |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ipaddr</i>        | IP address of the remote server.                                                                                                                                                                                                           |
| <i>hostname</i>      | Host name of the remote server.                                                                                                                                                                                                            |
| <i>facility-name</i> | <p>Name of a log facility:</p> <ul style="list-style-type: none"><li>• local0</li><li>• local1</li><li>• local2</li><li>• local3</li><li>• local4</li><li>• local5</li><li>• local6</li><li>• local7</li></ul> <p>There is no default.</p> |
| <i>port num</i>      | 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                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <i>max-messages</i> | Specifies the maximum number of messages the event log buffer will hold. The default buffer size (maximum messages) is 30000. |
| <b>disable</b>      | Disable logging to the monitor.                                                                                               |
| <b>emergency</b>    | Send emergency events (severity level 0—system unusable) to the monitor.                                                      |
| <b>alert</b>        | Send alert events (severity level 1—take action immediately) to the monitor.                                                  |
| <b>critical</b>     | Send critical events (severity level 2—system is in critical condition) to the monitor.                                       |
| <b>error</b>        | Send error events (severity level 3—system has an error condition) to the monitor.                                            |
| <b>warning</b>      | Send warning events (severity level 4—system has warning conditions) to the monitor.                                          |
| <b>notification</b> | Send notifications (severity level 5—normal but significant conditions) to the monitor.                                       |
| <b>information</b>  | Send informational messages (severity level 6) to the monitor.                                                                |
| <b>debugging</b>    | 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                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| <b>disable</b>      | Disable logging to the console.                                                         |
| <b>emergency</b>    | Send emergency events (severity level 0—system unusable) to the console.                |
| <b>alert</b>        | Send alert events (severity level 1—take action immediately) to the console.            |
| <b>critical</b>     | Send critical events (severity level 2—system is in critical condition) to the console. |
| <b>error</b>        | Send error events (severity level 3—system has an error condition) to the console.      |
| <b>warning</b>      | Send warning events (severity level 4—system has warning conditions) to the console.    |
| <b>notification</b> | Send notifications (severity level 5—normal but significant conditions) to the console. |
| <b>information</b>  | Send informational messages (severity level 6) to the console.                          |
| <b>debugging</b>    | 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                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>num</i>     | Specifies the maximum number of messages to buffer (16-256).<br><br>The default number is 50 messages.                                                                                                             |
| <i>minutes</i> | 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.<br><br>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] loggingemailfilter filter-num "conditions" operators`  
`[trigger]`

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>filter-num</i> | Specify the filter number (1-8).                                                                                                                                                                                                                                                                                                                                                                      |
| <i>conditions</i> | <p>Message attributes on which to match. The conditions list can contain one or more of the following:</p> <p>Severity levels of messages to send in email. Specify the severity levels by number or word:</p> <ul style="list-style-type: none"> <li>• 0 - emergency</li> <li>• 1 - alert</li> <li>• 2 - critical</li> <li>• 3 - error</li> <li>• 4 - warning</li> <li>• 5 - notification</li> </ul> |

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <ul style="list-style-type: none"> <li>• 6 - information</li> <li>• 7 - debugging</li> <li>• 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.</li> <li>• 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.</li> </ul>                                                                                                                                                                                                                                                                                                                                                      |
| <i>operators</i> | <p>Set of Boolean operators (AND, OR, NOT) that specify how the conditions should be compared.</p> <p>The CLI Boolean expression syntax is based on Reverse Polish Notation (also called Postfix Notation), a notation method that places an operator (AND, OR, NOT) after all of its operands (in this case, the conditions list).</p> <p>After listing all the conditions, specify the Boolean operator(s). The following operators are supported:</p> <ul style="list-style-type: none"> <li>• AND – All conditions must match in order for a log message to be emailed.</li> <li>• OR – Any one or more of the conditions must match in order for a log message to be emailed.</li> <li>• NOT – A log message is emailed only if it does not match the conditions</li> </ul> <p>For more information, see <a href="http://en.wikipedia.org/wiki/Reverse_Polish_notation">http://en.wikipedia.org/wiki/Reverse_Polish_notation</a> for Reverse Polish Notation</p> |



| Parameter            | Description                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>trigger</code> | Immediately sends the matching messages in an email instead of buffering them. If you omit this option, the messages are buffered based on the <a href="#">logging email buffer</a> 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 emailseverity-level
```

The *severity-level* can be one or more of the following (specify either the severity number or 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                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>address</i> | Email address to which event message will be sent.<br><br>To specify multiple Email addresses, use the <code>logging email-address</code> 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                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>all</code>           | Include system support messages.                                                                                                                      |
| <code>use-mgmt-port</code> | 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. |

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | Without this option, the ACOS device attempts to use the data route table to reach the remote device through a data interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <i>url</i> | <p>Saves a backup of the log to a remote server.</p> <p>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.</p> <p>The password can be up to 255 characters long and supports the following special characters:</p> <p>!#\$() *+,-. ;=^_`{ }~</p> <p>The following special characters are not supported:</p> <p>(blank space) "%&amp;'/:&lt;&gt;?@[\\]</p> <p>To enter the entire URL:</p> <ul style="list-style-type: none"> <li>• <code>tftp://host/file</code></li> <li>• <code>ftp://[user@]host[:port]/file</code></li> <li>• <code>scp://[user@]host/file</code></li> <li>• <code>sftp://[user@]host/file</code></li> </ul> |

**Default** Not set

**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 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                                                                                                                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>facility-name</i> | Name of a log facility: <ul style="list-style-type: none"><li>• local0</li><li>• local1</li><li>• local2</li><li>• local3</li><li>• local4</li><li>• local5</li><li>• local6</li><li>• local7</li></ul> |

**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. |

| Parameter                  | Description                                                              |
|----------------------------|--------------------------------------------------------------------------|
| <code>ipv6addr</code>      | IPv6 address of the syslog server.                                       |
| <code>hostname</code>      | Host name of the IPv4 syslog server.                                     |
| <code>ipv4addr</code>      | IPv4 address of the syslog server.                                       |
| <code>protocol-port</code> | Protocol port number to which to send messages (1-32767).                |
| <code>tcp</code>           | Use TCP as the transport protocol.                                       |
| <code>use-mgmt-port</code> | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <i>ip-based</i>   | Specify the LSN quota exceeded log based on private IP. This is disabled by default. Optionally, add RADIUS server attributes for logging using <code>with-radius-attribute</code> and at least one of the following parameters: <ul style="list-style-type: none"> <li><code>custom1</code>, <code>custom2</code>, <code>custom3</code> - Attribute not covered by other options. For more information, see “Customize RADIUS Attributes” in the <i>Traffic Logging Guide for IPV6 Migration</i>.</li> <li><code>imei</code> - International Mobile Equipment Identity (IMEI) attribute.</li> <li><code>imsi</code> - International Mobile Subscriber Identity (IMSI) attribute.</li> <li><code>msisdn</code> - Mobile Station International ISDN Number (MSISDN) attribute.</li> </ul> |
| <i>pool-based</i> | 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                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| <b>disable</b>      | Disable logging to the monitor.                                                         |
| <b>emergency</b>    | Send emergency events (severity level 0—system unusable) to the monitor.                |
| <b>alert</b>        | Send alert events (severity level 1—take action immediately) to the monitor.            |
| <b>critical</b>     | Send critical events (severity level 2—system is in critical condition) to the monitor. |
| <b>error</b>        | Send error events (severity level 3—system has an error condition) to the monitor.      |
| <b>warning</b>      | Send warning events (severity level 4—system has warning conditions) to the monitor.    |
| <b>notification</b> | Send notifications (severity level 5—normal but significant conditions) to the monitor. |
| <b>information</b>  | Send informational messages (severity level 6) to the monitor.                          |
| <b>debugging</b>    | 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                                                   |
|------------------|---------------------------------------------------------------|
| <b>emergency</b> | Log emergency events (severity level 0—system unusable) only. |
| <b>alert</b>     | Log alert events (severity level 1—take action                |



| Parameter           | Description                                                                  |
|---------------------|------------------------------------------------------------------------------|
|                     | immediately) only.                                                           |
| <b>critical</b>     | Log critical events (severity level 2—system is in critical condition) only. |
| <b>error</b>        | Log error events (severity level 3—system has an error condition) only.      |
| <b>warning</b>      | Log warning events (severity level 4—system has warning conditions) only.    |
| <b>notification</b> | Log notifications (severity level 5—normal but significant conditions) only. |
| <b>information</b>  | Log informational messages (severity level 6) only.                          |
| <b>debugging</b>    | 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                                                                                 |
|------------------|---------------------------------------------------------------------------------------------|
| <b>disable</b>   | Disable logging of syslog events.                                                           |
| <b>emergency</b> | Send emergency events (severity level 0—system unusable) to the syslog host.                |
| <b>alert</b>     | Send alert events (severity level 1—take action immediately) to the syslog host.            |
| <b>critical</b>  | Send critical events (severity level 2—system is in critical condition) to the syslog host. |
| <b>error</b>     | Send error events (severity level 3—system has an error condition) to the syslog host.      |

| Parameter           | Description                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------|
| <b>warning</b>      | Send warning events (severity level 4—system has warning conditions) to the syslog host.    |
| <b>notification</b> | Send notifications (severity level 5—normal but significant conditions) to the syslog host. |
| <b>information</b>  | Send informational messages (severity level 6) to the syslog host.                          |
| <b>debugging</b>    | 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                                                                               |
|------------------|-------------------------------------------------------------------------------------------|
| <b>disable</b>   | Disable logging of SNMP traps.                                                            |
| <b>emergency</b> | Sent emergency events (severity level 0—system unusable) to the SNMP host.                |
| <b>alert</b>     | Send alert events (severity level 1—take action immediately) to the SNMP host.            |
| <b>critical</b>  | 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 {source | dest | both}]`

| Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>mac-address</i>             | Hardware address, in the following format:<br><i>aabb.ccdd.eeff</i>                                                                                                                                                                                                                                                                                                                                                                     |
| <b>port</b><br><i>port-num</i> | ACOS Ethernet port to which to assign the MAC address.<br><br>If the ACOS device is a member of an aVCS virtual chassis, specify the interface as follows:<br><i>DeviceID/Portnum</i>                                                                                                                                                                                                                                                   |
| <b>vlan</b><br><i>vlan-id</i>  | Layer 2 broadcast domain in which to place the device.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>trap</b>                    | Send packets to the CPU for processing, instead of switching them in hardware.:<br><br><ul style="list-style-type: none"> <li>• <b>source</b> – Send packets that have this MAC as a source address to the CPU.</li> <li>• <b>dest</b> – Send packets that have this MAC as a destination address to the CPU.</li> <li>• <b>both</b> – Send packets that have this MAC as either a source or destination address to the CPU.</li> </ul> |

**NOTE:** The **trap** option is supported on only some AX models: AX 3200-12, AX 3400, AX 5200-11 and AX 5630.

**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.

|                |                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <code>[no] mac-age-time seconds</code> <p>Replace seconds with the number of seconds a learned MAC entry can remain unused before it is removed from the MAC table (10-600).</p>                                                                                                                                                                                                                       |
| <b>Default</b> | 300 seconds                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Mode</b>    | Configuration mode <p>On some AX 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.)</p> <p>On other models, the actual MAC aging time can be +/- 10 seconds from the configured value.</p> |
| <b>Example</b> | The following command changes the MAC aging time to 600 seconds:<br><pre>ACOS(config)# mac-age-time 600</pre>                                                                                                                                                                                                                                                                                          |

## maximum-paths

|                    |                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | Change the maximum number of paths a route can have in the Forwarding Information Base (FIB).                                                                                                                                                                                                      |
| <b>Syntax</b>      | <code>[no] maximum-paths num</code> <p>Replace <i>num</i> for the maximum number of paths a route can have. You can specify 1-64.</p>                                                                                                                                                              |
| <b>Default</b>     | 4                                                                                                                                                                                                                                                                                                  |
| <b>Mode</b>        | Global configuration                                                                                                                                                                                                                                                                               |
| <b>Usage</b>       | 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. |
| <b>Example</b>     | 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                                           |
|-----------------------------|-------------------------------------------------------|
| <code>server</code>         | Controls block-merge behavior for slb server.         |
| <code>service-group</code>  | Controls block-merge behavior for slb service-group.  |
| <code>virtual-server</code> | 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                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mirror-port</b><br><i>portnum</i> | Mirror port index number.                                                                                                                                                                                                                                                                                                                     |
| <b>ethernet</b><br><i>portnum</i>    | 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.                                                                                                                                                                                |
| <b>input</b>                         | Configures the mirror port so that only inbound traffic from the monitored port can be sent out of the mirror port.                                                                                                                                                                                                                           |
| <b>output</b>                        | Configures the mirror port so that only outbound traffic from the monitored port can be sent out of the mirror port.                                                                                                                                                                                                                          |
| <b>both</b>                          | Configures the mirror port so that both inbound and outbound traffic from the monitored port can be sent out of the mirror port.<br><br>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 <b>both</b> 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)# interface 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)# interface 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>resource-type</i> | <p>Type of resource for which to set the monitoring threshold:</p> <ul style="list-style-type: none"> <li>• <b>buffer-drop</b> – Packet drops (dropped IO buffers)</li> <li>• <b>buffer-usage</b> – Control buffer utilization</li> </ul> <p>The <b>conn-type</b> resources configure the conn resource type thresholds per CPU:</p> <ul style="list-style-type: none"> <li>• <b>conn-type0</b> – 32 bytes</li> <li>• <b>conn-type1</b> – 64 bytes</li> <li>• <b>conn-type2</b> – 128 bytes</li> </ul> |

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <ul style="list-style-type: none"> <li>• <b>conn-type3</b> – 256 bytes</li> <li>• <b>conn-type4</b> – 512 bytes</li> <li>• <b>ctrl-cpu</b> – Control CPU utilization</li> <li>• <b>data-cpu</b> – Data CPUs utilization</li> <li>• <b>disk</b> – Hard disk utilization</li> <li>• <b>memory</b> – Memory utilization</li> </ul> <p>The <b>smp-type</b> resources configure the Threshold for SMP resources for the global session memory pool, shared across all of the ACOS device's CPUs:</p> <ul style="list-style-type: none"> <li>• <b>smp-type0</b> – 32 bytes</li> <li>• <b>smp-type1</b> – 64 bytes</li> <li>• <b>smp-type2</b> – 128 bytes</li> <li>• <b>smp-type3</b> – 256 bytes</li> <li>• <b>smp-type4</b> – 512 bytes</li> <li>• <b>warn-temp</b> – CPU temperature</li> </ul> |
| <i>threshold-value</i> | 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

|                    |                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | Enable simultaneous admin sessions.                                                                                                                                                                                                                                                                                                        |
| <b>Syntax</b>      | <code>[no] multi-config enable</code>                                                                                                                                                                                                                                                                                                      |
| <b>Default</b>     | Enabled                                                                                                                                                                                                                                                                                                                                    |
| <b>Mode</b>        | Config                                                                                                                                                                                                                                                                                                                                     |
| <b>Usage</b>       | Use the “no” form of the command to disable multiple admin access.                                                                                                                                                                                                                                                                         |
| <b>NOTE:</b>       | 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

|                    |                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | To assign more than one CPU for control plane processing.                                                                                                                                                                                                                                                                                                 |
| <b>NOTE:</b>       | Not all devices support this command.                                                                                                                                                                                                                                                                                                                     |
| <b>Syntax</b>      | <code>multi-ctrl-cpu [num]</code><br><br>[num] is the required amount of control CPU.                                                                                                                                                                                                                                                                     |
| <b>Limitation</b>  | The number of control CPUs has the following limitations: <ul style="list-style-type: none"><li>• The number of control CPUs must be less than half of the total number of CPUs. This is calculated on a ratio basis.</li><li>• The maximum number of control CPUs is 8.</li><li>• The number of CPUs configured on vThunder must be 8 or more.</li></ul> |
| <b>Default</b>     | One CPU is used for control processing.                                                                                                                                                                                                                                                                                                                   |
| <b>Mode</b>        | Global configuration level                                                                                                                                                                                                                                                                                                                                |
| <b>Usage</b>       | This command enables the utilization of multiple CPUs for control plane processing. To view the number of CPUs statistics, use the <a href="#">show hardware</a> 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 |    |
| -----                    |      |       |       |       |    |
| Controll                 |      | 8%    | 9%    | 9%    | 9% |
| Data1                    |      | 0%    | 0%    | 0%    | 0% |
| Data2                    |      | 0%    | 0%    | 0%    | 0% |
| Data3                    |      | 0%    | 0%    | 0%    | 0% |
| Data4                    |      | 0%    | 0%    | 0%    | 0% |
| Data5                    |      | 0%    | 0%    | 0%    | 0% |
| I/O1                     |      | 0%    | 0%    | 0%    | 0% |
| I/O2                     |      | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>[no] custom-record options</code> | <p>Configure the custom record events to be exported:</p> <ul style="list-style-type: none"> <li>• <code>sesn-event-nat44-creation</code> – Export NAT44 session creation events</li> <li>• <code>sesn-event-nat44-deletion</code> – Export NAT44 session deletion events</li> <li>• <code>sesn-event-nat64-creation</code> – Export NAT64 session creation events</li> <li>• <code>sesn-event-nat64-deletion</code> – Export NAT64 session deletion events</li> <li>• <code>sesn-event-dslite-creation</code> – Export Dslite session creation events</li> <li>• <code>sesn-event-dslite-deletion</code> – Export Dslite session deletion events</li> <li>• <code>sesn-event-fw4-creation</code> – Export FW4 session creation events</li> <li>• <code>sesn-event-fw4-deletion</code> – Export FW4 session deletion events</li> <li>• <code>sesn-event-fw6-creation</code> – Export FW6 session creation events</li> <li>• <code>sesn-event-fw6-deletion</code> – Export FW6 session deletion events</li> <li>• <code>deny-reset-event-fw4</code> – Export FW4 Deny Reset events</li> <li>• <code>deny-reset-event-fw6</code> – Export FW6 Deny Reset events</li> <li>• <code>port-mapping-nat44-creation</code> – Export NAT44 Port Mapping Creation Event</li> <li>• <code>port-mapping-nat44-deletion</code> – Export NAT44 Port Mapping Deletion Event</li> </ul> |

| Command                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               | <ul style="list-style-type: none"> <li>• port-mapping-nat64-creation – Export NAT64 Port Mapping Creation Event</li> <li>• port-mapping-nat64-deletion – Export NAT64 Port Mapping Deletion Event</li> <li>• port-mapping-dslite-creation – Export Dslite Port Mapping Creation Event</li> <li>• port-mapping-dslite-deletion – Export Dslite Port Mapping Deletion Event</li> <li>• port-batch-nat44-creation – Export NAT44 Port Batch Creation Event</li> <li>• port-batch-nat44-deletion – Export NAT44 Port Batch Deletion Event</li> <li>• port-batch-nat64-creation – Export NAT64 Port Batch Creation Event</li> </ul>                                                                                               |
| <b>[no] custom-record</b><br><i>options</i><br><i>(cont.)</i> | <ul style="list-style-type: none"> <li>• port-batch-nat64-deletion – Export NAT64 Port Batch Deletion Event</li> <li>• port-batch-dslite-creation – Export Dslite Port Batch Creation Event</li> <li>• port-batch-dslite-deletion – Export Dslite Port Batch Deletion Event</li> <li>• port-batch-v2-nat44-creation – Export NAT44 Port Batch v2 Creation Event</li> <li>• port-batch-v2-nat44-deletion – Export NAT44 Port Batch v2 Deletion Event</li> <li>• port-batch-v2-nat64-creation – Export NAT64 Port Batch v2 Creation Event</li> <li>• port-batch-v2-nat64-deletion – Export NAT64 Port Batch v2 Deletion Event</li> <li>• port-batch-v2-dslite-creation – Export Dslite Port Batch v2 Creation Event</li> </ul> |

| Command                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                        | <ul style="list-style-type: none"> <li>port-batch-v2-dslite-deletion – Export Dslite Port Batch v2 Deletion Event</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>[no] destination<br/>ipaddr<br/>[portnum]</code> | Configure the destination where NetFlow records will be sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>disable</code>                                   | Disable this NetFlow monitor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>[no] flow-<br/>timeout</code>                    | <p>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.</p> <p>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.</p> <hr/> <p><b>NOTE:</b> Apart from flow records (in case of fixed templates) this statement holds true for session deletion records (in case of custom records) as well.</p> <hr/> <p>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.</p> |
| <code>[no] protocol</code>                             | <p>Configure the version of the NetFlow protocol you want to use:</p> <ul style="list-style-type: none"> <li>v9 – Version 9 (default)</li> <li>v10 – Version 10 (IPFIX)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>[no] record</code>                               | Configure the NetFlow record types to be exported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



| Command                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>netflow-template-type</code> | <ul style="list-style-type: none"> <li>• <code>dslite</code> – Export DS-Lite Flow Record Template</li> <li>• <code>nat44</code> – Export NAT44 Flow Record Template</li> <li>• <code>nat64</code> – Export NAT64 Flow Record Template</li> <li>• <code>netflow-v5</code> – Export NetFlow V5 Flow Record Template</li> <li>• <code>netflow-v5-ext</code> – Export extended NetFlow V5 Flow Record Template, supports ipv6</li> <li>• <code>port-batch-dslite</code> – Export DS-Lite Port Batching Event Template</li> <li>• <code>port-batch-nat44</code> – Export NAT44 Port Batching Event Template</li> <li>• <code>port-batch-nat64</code> – Export NAT64 Port Batching Event Template</li> <li>• <code>port-batch-v2-dslite</code> – Export DS-Lite NAT Port Batching v2 Event Template</li> <li>• <code>port-batch-v2-nat44</code> – Export NAT44 NAT Port Batching v2 Event Template</li> <li>• <code>port-batch-v2-nat64</code> – Export NAT64 NAT Port Batching v2 Event Template</li> <li>• <code>port-mapping-dslite</code> – Export DS-Lite Port Mapping Event Template</li> <li>• <code>port-mapping-nat44</code> – Export NAT44 Port Mapping Event Template</li> <li>• <code>port-mapping-nat64</code> – Export NAT64 Port Mapping Event Template</li> <li>• <code>sesn-event-dslite</code> – Export DS-Lite Session Event Template</li> <li>• <code>sesn-event-fw4</code> – Export FW Ipv4 Session Event Template</li> </ul> |

| Command                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <ul style="list-style-type: none"> <li>• <code>sesn-event-fw6</code> – Export FW Ipv6 Session Event Template</li> <li>• <code>sesn-event-nat44</code> – Export NAT44 Session Event Template</li> <li>• <code>sesn-event-nat64</code> – Export NAT64 Flow Record Template</li> </ul> <p>For more information, see “NetFlow v9 and v10 (IPFIX)” chapter in the <i>System Configuration and Administration Guide</i>.</p>                                                                                                                                                                                                           |
| <pre>[no] resend- template {records num     timeout seconds}</pre> | <p>Configure when to resend the NetFlow template. The trigger can be either the number of records, or the amount of time that has passed.</p> <ul style="list-style-type: none"> <li>• <b>records</b> – Specifies the counters by which the ACOS device resends templates to the collectors. The <i>num</i> can be 0-1000000. The default is 1000.</li> <li>• <b>timeout</b> – Specifies the time between when templates are resent to the collectors. The <i>num</i> is the number of seconds and can be 0-86400. The default is 1800.</li> </ul> <hr/> <p><b>NOTE:</b> Specifying 0 means never resend the template.</p> <hr/> |
| <pre>[no] sample {ethernet   global   nat-pool   ve}</pre>         | <p>Enable sampling.</p> <p>Configure filters for monitoring traffic. Identify the specific type and subset of resources to monitor.</p> <ul style="list-style-type: none"> <li>• <b>ethernet</b> <i>portnum</i> – Specify the list of Ethernet data ports to monitor. Flow information for the monitored interfaces is sent to the NetFlow collector(s).</li> <li>• <b>global</b> – (Default) No filters are in effect. Traffic on all interfaces is monitored.</li> </ul>                                                                                                                                                       |

| Command                                                                                            | Description                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                    | <ul style="list-style-type: none"> <li>• <b>nat-pool</b> <i>pool-name</i> – NAT pool.</li> <li>• <b>ve</b> <i>ve-num</i> – Specify the list of Virtual Ethernet (VE) data ports to monitor.</li> </ul>                                         |
| <b>[no] source-address</b><br>{ <b>ip</b><br><i>ipv4addr</i>  <br><b>ipv6</b><br><i>ipv6addr</i> } | 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. |
| <b>[no] source-ip-use-mgmt</b>                                                                     | 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.                                                               |
| <b>[no] user-tag</b><br><i>user-tag-name</i>                                                       | Custom tag that can then be searched by using the aXAPI.                                                                                                                                                                                       |
| <b>[no] disable-log-by-destination</b>                                                             | Command in netflow monitor configuration mode are available for disabling of logging by destination protocol and port.<br><br>Following are the sub-commands under this mode.                                                                  |
| <b>[no] icmp</b>                                                                                   | Disable logging for ICMP traffic.                                                                                                                                                                                                              |
| <b>[no] others</b>                                                                                 | Disable logging for L4 protocol traffic that is not TCP or UDP.                                                                                                                                                                                |
| <b>[no] tcp</b>                                                                                    | Disable logging for TCP traffic.                                                                                                                                                                                                               |
| <b>[no] udp</b>                                                                                    | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>[no]<br/>information-<br/>element<br/>options</code> | Command in NetFlow template configuration mode that places you in a sub-configuration mode, where the commands in <a href="#">Table 11</a> are available for configuring one or more information elements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>[no]<br/>template-id<br/>num</code>                  | <p>Configure the custom IPFIX Template ID. The <i>num</i> can be 2001-3000.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.]</li> </ul> |

Table 11 : 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)  |
| 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)                 |

Table 11 : Sub-Commands in the netflow template information-element Configuration Mode

| Command              | Description                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------|
| 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)                                     |
| 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)                                |

Table 11 : Sub-Commands in the netflow template information-element Configuration Mode

| Command                      | Description                                                      |
|------------------------------|------------------------------------------------------------------|
| 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-subcategory-name | Application second level category name (ID: 373)                 |
| 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)  |

Table 11 : Sub-Commands in the netflow template information-element Configuration Mode

| Command               | Description                                                                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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                                                                                                                                                                                     |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>[no] use-partition <i>partition-name</i></code> | Specify the dedicated partition name to send the NetFlow logs.<br><br><b>NOTE:</b> You cannot configure <code>netflow use-partition</code> 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>disable</b>                                                   | Disables synchronization with the NTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>enable</b>                                                    | Enables synchronization with the NTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>key</b> <i>ID-num</i>                                         | Creates an authentication key. For <i>ID-num</i> , enter a value between 1-65535.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>prefer</b>                                                    | Directs ACOS to use this NTP server by default. Additional NTP servers are used as backup servers if the preferred NTP server is unavailable.                                                                                                                                                                                                                                                                                                                                                    |
| <b>{M   SHA   SHA1}</b><br><b>{ascii   hex}</b><br><i>string</i> | <p>Specifies the type of authentication key you want to create for authenticating the NTP servers.</p> <ul style="list-style-type: none"> <li>• <b>M</b> - encryption using MD5</li> <li>• <b>SHA</b> - encryption using SHA</li> <li>• <b>SHA1</b> - encryption using SHA1</li> </ul> <p>Specify the authentication key <i>string</i> (1-20 characters). Use the <b>hex</b> parameter to specify the <i>string</i> in hex format (21-40 characters), or <b>ascii</b> to specify it in text.</p> |
| <b>trusted-key</b> <i>ID-num</i>                                 | Adds an authentication key to the list of trusted keys. For <i>num</i> , 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>group-name</i> | Name of the network object group (1-63 characters).                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>acl</b>        | Create a network object group that will be used by Access Control Lists.<br><br>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 do not need to edit each individual ACL. |
| <b>fw v4</b>      | Create a network object group that will be used for IPv4 firewall configurations.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>f4 v6</b>      | 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                                                                                                                                                                                |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[no] any</b>                | Matches on all IP addresses.                                                                                                                                                               |
| <b>[no] description string</b> | Description (1-128 characters) of the object group instance being configured.<br><br>The description string can be any combination of letters and numbers and is common for all objects in |

| Command                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                      | the group. You can specify the <i>group-name</i> of the object group in the description.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>[no]</b><br><b>host</b> <i>host-src-ipaddr</i>                                    | Matches only on the specified host IPv4 or IPv6 address.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>[no]</b> <i>net-src-ipaddr {</i><br><i>filter-mask  </i><br><i>/mask-length }</i> | Matches on any host in the specified IPv4 subnet.<br><br>The <i>filter-mask</i> specifies the portion of the address to filter:<br><ul style="list-style-type: none"> <li>• Use 0 to match.</li> <li>• Use 255 to ignore.</li> </ul> For example, the following <i>filter-mask</i> filters on a 24-bit subnet: 0.0.0.255<br><br>Alternatively, you can use <i>mask-length</i> 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. |
| <b>[no]</b> <i>net-src-ipv6addr</i><br><i>/prefix-length</i>                         | Matches on any host in the specified subnet. The <i>prefix-length</i> specifies the portion of the address to filter.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>[no]</b><br><i>sequence-number</i>                                                | 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] <b>description</b> <i>string</i>    | Description (1-128 characters) of the object group instance being configured.<br><br>The description string can be any combination of letters and numbers and is common for all objects in the group. You can specify the <i>group-name</i> of the object group in the description. |
| [no] <b>icmp</b><br>[ <b>type</b> {type- | Matches on ICMP traffic.                                                                                                                                                                                                                                                            |

| Command                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>option} [code {any- code   code- num}]]</pre> | <p>The <b>type</b> <i>type-option</i> parameter matches based on the specified ICMP type. You can specify one of the following ICMP types (enter either the number or the name):</p> <ul style="list-style-type: none"> <li>• <b>any-type</b> – Matches on any ICMP type.</li> <li>• <b>dest-unreachable</b>   3 – Type 3, destination unreachable</li> <li>• <b>echo-reply</b>   0 – Type 0, echo reply</li> <li>• <b>echo-request</b>   8 – Type 8, echo request</li> <li>• <b>info-reply</b>   16 – Type 16, information reply</li> <li>• <b>info-request</b>   15 – Type 15, information request</li> <li>• <b>mask-reply</b>   18 – Type 18, address mask reply</li> <li>• <b>mask-request</b>   17 – Type 17, address mask request</li> <li>• <b>parameter-problem</b>   12 – Type 12, parameter problem</li> <li>• <b>redirect</b>   5 – Type 5, redirect message</li> <li>• <b>source-quench</b>   4 – Type 4, source quench</li> <li>• <b>time-exceeded</b>   11 – Type 11, time exceeded</li> <li>• <b>timestamp</b>   13 – Type 13, timestamp</li> <li>• <b>timestamp-reply</b>   14 – Type 14, timestamp reply</li> </ul> <p>The <b>code</b> <i>code-num</i> option is applicable if the protocol type is <b>icmp</b>. You can specify:</p> <ul style="list-style-type: none"> <li>• <b>any-code</b> – Matches on any ICMP code.</li> <li>• <b>code-num</b> – ICMP code number, 0-254</li> </ul> |

| Command                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>[no] icmpv6 [type {type- option} [code {any- code   code- num}]]</pre> | <p>Matches on ICMPv6 traffic.</p> <p>The <b>type</b> <i>type-option</i> parameter matches based on the specified ICMPv6 type. You can specify one of the following types (enter either the number or the name):</p> <p><b>any-type</b> – Matches on any ICMPv6 type.</p> <ul style="list-style-type: none"> <li>• <b>dest-unreachable</b> – Matches on type 1, destination unreachable messages.</li> <li>• <b>echo-reply</b> – Matches on type 129, echo reply messages.</li> <li>• <b>echo-request</b> – Matches on type 128, echo request messages.</li> <li>• <b>packet-too-big</b> – Matches on type 2, packet too big messages.</li> <li>• <b>param-prob</b> – Matches on type 4, parameter problem messages.</li> <li>• <b>time-exceeded</b> – Matches on type 3, time exceeded messages.</li> </ul> |
| <pre>[no] protocol- id id</pre>                                             | <p>Specify the protocol ID on which to match.</p> <p>For more information, see <a href="https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers">https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers</a> for a list of protocol IDs and corresponding protocols.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>{tcp   udp} eq src-port   gt src-port   lt src-port  </pre>            | <p>Specifies the protocol ports on which to match:</p> <ul style="list-style-type: none"> <li>• <b>eq</b> <i>src-port</i> – The ACL matches on traffic on the specified port.</li> <li>• <b>gt</b> <i>src-port</i> – The ACL matches on traffic on any port with a higher number than the specified port.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



| Command                                                   | Description                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>range</b> <i>start-src-port</i><br><i>end-src-port</i> | <ul style="list-style-type: none"> <li>• <b>lt</b> <i>src-port</i> – The ACL matches on traffic on any port with a lower number than the specified port.</li> <li>• <b>range</b> <i>start-src-port</i> <i>end-src-port</i> – The ACL matches on traffic on any port within the specified range.</li> </ul> |

**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                   |
|--------------------|-------------------------------|
| <code>trap</code>  | Trap packets to the CPU.      |
| <code>flood</code> | 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, 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>hostname   ipaddr</i> | <p>Hostname or IP address of the RADIUS server.</p> <p><b>secret secret-string</b>[options]: Password, 1-128 characters, required by the RADIUS server for authentication requests.</p> <p>The following protocol options are used to manage RADIUS communication:</p> <ul style="list-style-type: none"> <li>• <b>acct-port</b><i>protocol-port</i>: Protocol port to which the ACOS device sends RADIUS accounting information. The default port is 1813.</li> <li>• <b>auth-port</b><i>protocol-port</i>:</li> </ul> |

| Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <p>Protocol port to which the ACOS device sends authentication requests.</p> <p>The default port is 1812.</p> <ul style="list-style-type: none"> <li>• <b>retransmit num</b>: 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.</li> </ul> <p>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 admin is denied access.</p> <p>You can specify 0-5 retries. The default is 3 retries.</p> <ul style="list-style-type: none"> <li>• <b>timeoutseconds</b>: 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.</li> </ul> <p>The default is 3 seconds.</p> |
| <b>default-privilege-read-write</b> | Change the default privilege authorized by RADIUS from read-only to read-write. The default                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Parameter                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | <p>privilege is used if the Service-Type attribute is not used, or the A10 vendor attribute is not used.</p> <p>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.</p>                                                                                                                                                                                                                                        |
| <code>message-authenticator-verify-enable</code> | <p>Enables the verification of the Message-Authenticator attribute in RADIUS messages.</p> <p>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.</p> <p>When this is disabled, responses without the attribute will still be accepted for compatibility.</p> <p><b>NOTE:</b> It is recommended to enable this field and configure the RADIUS server to support the Message-Authenticator attribute for enhanced security.</p> |

**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] <code>bgp</code> | 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. |

| Parameter            | Description                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[no] gateway</b>  | 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. |
| <b>[no] ethernet</b> | 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.                                        |
| <b>[no] route</b>    | If an IPv4 or IPv6 route matching the specified options is not in the data route table, the cost of the event increases.                                                                                                                                                   |
| <b>[no] trunk</b>    | If the trunk or individual ports in the trunk go down, the cost of the event increases.                                                                                                                                                                                    |
| <b>[no] VLAN</b>     | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>use-mgmt-port</code> | 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.                                                                                                                                                                                                                                                                                                          |
| <code>url</code>           | <p>File transfer protocol, username (if required), and directory path.</p> <p>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.</p> <p>The password can be up to 255 characters long and supports the following special characters:</p> <pre>!#\$()*+,-.;=^_`{ }~</pre> <p>The following special characters are not supported:</p> <pre>(blank space) "%&amp;'/:;&lt;&gt;?@[\\</pre> <p>To enter the entire URL:</p> |

| Parameter | Description                                                                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <ul style="list-style-type: none"> <li>• <code>tftp://host/file</code></li> <li>• <code>ftp://[user@]host[:port]/file</code></li> <li>• <code>scp://[user@]host/file</code></li> <li>• <code>sftp://[user@]host/file</code></li> </ul> |

**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                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>map-name</i>             | Route map name.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>deny</b>   <b>permit</b> | Action to perform on data that matches the rule.                                                                                                                                                                                                                                                                                                                                        |
| <i>sequence-num</i>         | <p>Sequence number of the rule within the route map, 1-65535. Rules are used in ascending sequence order.</p> <p>The action in the first matching rule is used, and no further matching is performed.</p> <p>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.</p> |

This command changes the CLI to the configuration level for the specified route map rule, where the following commands are available.

| Command                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>match</code><br><i>attribute</i> | <p>Specifies the match criteria for routes:</p> <ul style="list-style-type: none"> <li>• <b>match as-path</b> <i>list-id</i> – Matches on the BGP AS paths in the specified AS path list.</li> <li>• <b>match community</b> <i>list-id1</i> [<i>list-id2 ... list-idn</i>] – Matches on the BGP communities in the specified community list. When the command specifies multiple lists, the route must match on each list.</li> <li>• <b>match extcommunity</b> <i>list-id1</i> [<i>list-id2 ... list-idn</i>] – 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.</li> <li>• <b>match group</b> <i>num</i> {<b>active</b>   <b>standby</b>} – Matches on VRRP-A set ID and state (active or standby).</li> <li>• <b>match interface</b> {<b>ethernet</b> <i>portnum</i>   <b>loopback</b> <i>num</i>   <b>trunk</b> <i>num</i>   <b>ve</b> <i>ve-num</i>} – Matches on the data interface used as the first hop for a route.</li> <li>• <b>match ip address</b> {<i>acl-id</i>   <b>prefix-list</b> <i>list-name</i>} – Matches on the route IP addresses in the specified ACL or prefix list.</li> <li>• <b>match ip next-hop</b> {<i>acl-id</i>   <b>prefix-list</b> <i>list-name</i>} – Matches on the next-hop router IP addresses in the specified ACL or prefix list.</li> <li>• <b>match ip peer</b> <i>acl-id</i> – Matches on the peer router IP addresses in the specified list.</li> <li>• <b>match ipv6 address</b> {<i>acl-id</i>   <b>prefix-list</b> <i>list-name</i>} – Matches on the route IP addresses in the specified ACL or prefix list.</li> </ul> |

| Command                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <ul style="list-style-type: none"> <li>• <b>match ipv6 next-hop</b> <i>{acl-id   prefix-list list-name   ipv6-addr}</i> – Matches on the next-hop router IP addresses in the specified ACL or prefix list, or the specified IPv6 address.</li> <li>• <b>match ipv6 peer</b> <i>acl-id</i> [<b>exact-match</b>]– Matches on the BGP communities listed in the specified large community list.</li> <li>• <b>match large community</b><i>list-id</i> [<b>exact-match</b>]– Matches on the BGP communities listed in the specified large community list.</li> <li>• <b>match local-preference</b> <i>num</i> – Matches on the specified local preference value, 0-4294967295.</li> <li>• <b>match metric</b> <i>num</i> – Matches on the specified route metric value, 0-4294967295.</li> <li>• <b>match origin</b> <i>{egp   igp   incomplete}</i> – Matches on the specified BGP origin code.</li> <li>• <b>match route-type external</b> <i>{type-1   type-2}</i> – Matches on the specified external route type.</li> <li>• <b>match scaleout</b> <i>cluster-id</i> – Matches on the specified scaleout status.</li> <li>• <b>match tag</b> <i>tag-value</i> – Matches on the specified TAG value, 0-4294967295.</li> </ul> |
| <b>set</b><br><i>attribute</i> | <p>Sets information for matching routes:</p> <ul style="list-style-type: none"> <li>• <b>set aggregator as</b> <i>as-num ipaddr</i> – Sets the aggregator attribute.</li> <li>• <b>set as-path prepend</b> <i>as-num [...]</i> – Adds the specified BGP AS number(s) to the front of the AS-path attribute.</li> <li>• <b>set atomic-aggregate</b> – Specifies that a BGP route has been aggregated, and that path information for</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Command | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>the individual routes that were aggregated together is not available.</p> <ul style="list-style-type: none"> <li>• <b>set comm-list</b> <i>list-id</i> <b>delete</b> – Sets the specified BGP community list to be deleted.</li> <li>• <b>set community</b> <i>community-value</i> – Sets the BGP community ID to the specified value: <ul style="list-style-type: none"> <li>◦ <b>&lt;1-4294967295&gt;</b> – Sets the community number.</li> <li>◦ <b>AS:NN</b>, where <i>AS</i> is the AS number and <i>NN</i> is a numeric value in the range 1-4294967295.</li> <li>◦ <b>internet</b> – Internet route.</li> <li>◦ <b>local-AS</b> – Advertises routes only within the local Autonomous System (AS), not to external BGP peers.</li> <li>◦ <b>no-advertise</b> – Does not advertise routes.</li> <li>◦ <b>no-export</b> – Does not advertise routes outside the AS boundary.</li> <li>◦ <b>none</b> – No community attribute.</li> </ul> </li> <li>• <b>set dampening</b> [<i>reachability-half-life</i> [<i>reuse-value</i> [<i>suppress-value</i>] [<i>max-duration</i> [<i>unreachability-half-life</i>]]]] – Enables route-flap dampening. Route-flap dampening helps minimize network instability caused by unstable routes.</li> <li>• <i>reachability-half-life</i> – 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.</li> <li>• <i>reuse-value</i> [<i>suppress-value</i>] – Penalty thresholds for the suppression and reuse (re-advertisement) of a route. The supported range for</li> </ul> |

| Command                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <p>each value is 1-20000. The default <i>suppress-value</i> is 2000. the default <i>reuse-value</i> is 750.</p> <ul style="list-style-type: none"> <li>• <i>max-duration</i> – Maximum amount of time a route will remain suppressed, 1-255 minutes. The default is 4 times the <i>reachability-half-life</i>.</li> <li>• <i>unreachability-half-life</i> – <i>Unreachability</i> 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.</li> </ul> <p>(cont.)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>set</b><br><i>attribute</i> | <ul style="list-style-type: none"> <li>• <b>set extcommunity</b> <i>comm-id</i> [...] – Sets the BGP extended community attribute.</li> <li>• <b>set ip next-hop</b> <i>ipaddr</i> – Sets the next hop for matching IPv4 routes.</li> <li>• <b>set ipv6</b> [<i>local</i>] <i>ipv6addr</i> – Set the next hop for matching IPv6 routes. If the address is for an inside network (not globally routable), use the <i>local</i> option.</li> <li>• <b>set large-comm-list</b> <i>list-id</i> <b>delete</b> – Sets the specified BGP large community list to be deleted.</li> <li>• <b>set large-community</b> <i>community-value</i> – Sets the BGP Large community ID to the specified value: <ul style="list-style-type: none"> <li>◦ <b>NAME</b>&lt;length:1-128&gt; – Sets the large community number in the xx:yy:zz format.</li> <li>◦ <b>none</b> – No community attribute.</li> </ul> </li> <li>• <b>set level</b> {<i>level-1</i>   <i>level-1-2</i>   <i>level-2</i>} – Sets the IS-IS level for exporting a route to IS-IS.</li> <li>• <b>set local-preference</b> <i>num</i> – Sets the BGP local preference path attribute.</li> <li>• <b>set metric</b> <i>metric-value</i> – Sets the metric value for the destination routing protocol.</li> </ul> |



| Command | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"> <li>• <b>set metric-type</b> {<b>external</b>   <b>internal</b>   <b>type-1</b>   <b>type-2</b>} – Sets the metric type for the destination routing protocol.</li> <li>• <b>set origin</b> {<b>egp</b>   <b>igp</b>   <b>incomplete</b>} – Sets the origin attribute: <ul style="list-style-type: none"> <li>◦ <b>egp</b> – Exterior gateway protocol.</li> <li>◦ <b>igp</b> – Interior gateway protocol.</li> <li>◦ <b>incomplete</b> – Unknown heritage.</li> </ul> </li> <li>• <b>set originator-id</b> <i>ipaddr</i> – Sets the BGP originator attribute.</li> <li>• <b>set tag</b> <i>tag-value</i> – Sets the tag value for the destination routing protocol.</li> <li>• <b>set weight</b> <i>num</i> – Sets the BGP weight value for the routing table.</li> </ul> |

|                |                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------|
| <b>Default</b> | None                                                                                                    |
| <b>Mode</b>    | Configuration mode                                                                                      |
| <b>Usage</b>   | 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                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bgp</b> <i>AS-num</i> | Specifies an Autonomous System (AS) for which to run Border Gateway Protocol (BGP) on the ACOS device. This also enters BGP configuration mode. |

| Command                                                       | Description                                                                                                                                                                     |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b> { <b>ospf</b><br>[ <i>tag</i> ]  <br><b>rip</b> } | 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. |
| <b>isis</b> [ <i>tag</i> ]                                    | Enter configuration mode for Intermediate System to Intermediate System (IS-IS).                                                                                                |
| <b>ospf</b><br>[ <i>process-id</i> ]                          | Specifies an IPv4 OSPFv2 process (1-65535) to run on the ACOS device, and also enter OSPF configuration mode.                                                                   |
| <b>rip</b>                                                    | 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                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------|
| <b>name</b><br><i>string</i> | Name of the log file.                                                                              |
| <b>per-protocol</b>          | Uses separate log files for each protocol. Without this option, log messages for all protocols are |

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | written to the same file.<br><br>By default, this is disabled.                                                                                                                                                                                                                                                                       |
| <b>rotate</b><br><i>num</i>  | 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.<br><br>The default is 0. |
| <b>size</b><br><i>Mbytes</i> | Specifies the size of each log file. You can specify 0-1000000 Mbytes. If you specify 0, the file size is unlimited.<br><br>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.

**NOTE:** 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. Currently, the hardware diagnostics menu is supported in AX Release 2.4.3-P3 and later 2.4.x releases, and in AX Release 2.6.1.

**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

000000000000

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                                  |
|-------------------|----------------------------------------------|
| <b>aflex</b>      | Show aFlex scripts in the running-config.    |
| <b>class-list</b> | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dest-addr</b><br><b>dest-port</b><br><b>source-addr</b><br><b>source-port</b> | <p>Matches on sessions that have a source or destination IPv4 address or port:</p> <ul style="list-style-type: none"> <li>• <b>source-addr</b> <i>ipaddr</i> [{<i>subnet-mask</i>   /<i>mask-length</i>}] – Matches on IPv4 sessions that have the specified source IP address.</li> <li>• <b>source-port</b> <i>port-num</i> – Matches on IPv4 sessions that have the specified source protocol port number, 1-65535.</li> <li>• <b>dest-addr</b> – Matches on IPv4 sessions that have the specified destination IP address.</li> <li>• <b>dest-port</b> – Matches on IPv4 sessions that have the specified destination protocol port number, 1-65535.</li> </ul> <p>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 <b>dest-addr</b>, the only additional suboption you can specify is <b>dest-port</b>.</p> |
| <b>ipv6</b>                                                                      | Matches on all sessions that have a source or                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Parameter  | Description                  |
|------------|------------------------------|
|            | destination IPv6 address.    |
| <b>sip</b> | 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 | Reverse |
|------|-----------------|--------------|----------------|-----------------|-----|------|---------|
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>agent</b><br><b>address</b><br>{ <i>ipaddr</i>   <i>ipv6addr</i> }                                                                    | Configure an sFlow agent. The <i>ipaddr</i> 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.                                                                                                                                                                           |
| <b>collector</b><br>{ <b>ip</b> <i>ipaddr</i>   <b>ipv6</b> <i>ipv6addr</i> }<br><i>portnum</i>                                          | 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.<br><br>The default port number is 6343.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>polling</b><br><i>type</i>                                                                                                            | 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: <ul style="list-style-type: none"> <li>• <b>cpu-usage</b> – Polls for CPU utilization statistics.</li> <li>• <b>ethernet</b> – Polls for Ethernet data interface statistics.</li> <li>• <b>http-counter</b> - Polls for HTTP statistics.</li> <li>• <b>ve</b> - Polls for statistics for Virtual Ethernet (VE) interfaces.</li> </ul> All sFlow polling (collection) is disabled by default |
| <b>sampling</b><br>{ <b>ethernet</b> <i>portnum</i> [ <b>to</b> <i>portnum</i> ]   <b>ve</b> <i>ve-num</i> [ <b>to</b> <i>ve-num</i> ] } | Enable sFlow sampling on a specified interface.<br><br>There is no default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>setting</b><br><i>sub-</i>                                                                                                            | Configure global sFlow settings:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>options</i> | <ul style="list-style-type: none"> <li>• <b>counter-polling-interval</b> <i>seconds</i> – Configure the sFlow counter polling interval. The <b>interval</b> <i>seconds</i> 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.</li> <li>• <b>local-collection</b> – Configure the local sFlow collection. <ul style="list-style-type: none"> <li>◦ <b>enable</b> – Enable local sFlow collection.</li> <li>◦ <b>disable</b> – Disable local sFlow collection.</li> </ul> </li> </ul> <hr/> <p><b>NOTE:</b> 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.</p> <hr/> <ul style="list-style-type: none"> <li>• <b>max-header</b> <i>bytes</i> – Maximum number of bytes to sample from any given packet, 14-512 bytes. The default is 128 bytes.</li> <li>• <b>packet-sampling-rate</b> <i>num</i> – Configure sFlow default packet sampling rate. The <i>num</i> option specifies the value of <i>N</i>, where <i>N</i> 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.</li> <li>• <b>source-ip-use-mgmt</b> – Enable use of the management interface's IP as the source address for outbound sFlow packets.</li> </ul> |
| <b>source-</b> | Source IP address for sFlow packets sent from ACOS to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Parameter                                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>address</b><br>{ <b>ip</b> <i>ipaddr</i><br>  <b>ipv6</b><br><i>ipv6addr</i> } | <p>sFlow collectors.</p> <p>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.</p> |

**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, 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                                                                                          |
|------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <i>hostname   ipaddr</i>                       | Configure a name or IP address for the SMTP server.                                                  |
| <i>mailfrom email-src-addr</i>                 | Specifies the email address to use as the sender (From) address.                                     |
| <i>needauthentication</i>                      | Specifies that authentication is required.<br>This is disabled by default.                           |
| <i>port protocol-port</i>                      | Specifies the protocol port on which the server listens for SMTP traffic.<br>The default port is 25. |
| <i>server hostname</i>                         | Configure a name for the SMTP server.                                                                |
| <i>username name</i><br><i>password string</i> | 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

### 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(config)# snmp-server 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                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>  | Enables all the traps described below.<br><br><b>NOTE:</b> The <b>all</b> option can be specified at any command level to enable all SNMP traps at that level.                                                                                                                                       |
| <b>gslb</b> | Enables GSLB group traps: <ul style="list-style-type: none"> <li>• <b>group</b> – Enable group-related traps.</li> <li>• <b>service-ip</b> – Enable traps related to service-IPs.</li> <li>• <b>site</b> – Enable site-related traps.</li> <li>• <b>zone</b> – Enable zone-related traps.</li> </ul> |
| <b>lldp</b> | Enables LLDP group traps.                                                                                                                                                                                                                                                                            |
| <b>lsn</b>  | Enables LSN group traps: <ul style="list-style-type: none"> <li>• <b>fixed-nat-port-mapping-file-change</b> - Enables LSN</li> </ul>                                                                                                                                                                 |

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <p>trap when the fixed NAT port mapping file changes).</p> <ul style="list-style-type: none"> <li>• <b>per-ip-port-uage-threshold</b> - Enables LSN trap when IP total port usage reaches the threshold.</li> <li>• <b>total-port-usage-threshold</b> - Enables LSN trap when NAT total port usage reaches the threshold.</li> <li>• <b>traffic-exceeded</b> - Enables LSN trap when NAT pool reaches the threshold.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>network</b> | <p>Enables network group traps:</p> <ul style="list-style-type: none"> <li>• <b>trunk-port-threshold</b> – 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.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>routing</b> | <p>Enables the routing group traps:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b> – Enables traps for BGP routing. BGP traps for IPv4 address family as defined in rfc4273: <ul style="list-style-type: none"> <li>◦ <b>bgpEstablishedNotification</b> - A BGP neighbor transitions to the Established state.</li> <li>◦ <b>bgpBackwardTransNotification</b> - 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.</li> </ul> <p>BGP traps for IPv4 and IPv6 address families as defined in AX-BGP-MIB proprietary MIB:</p> <li>◦ <b>bgp ax</b> - Enables AX-BGP-MIB traps for IPv4 and IPv6 families: <ul style="list-style-type: none"> <li>■ <b>bgpEstablishedNotification</b> - A BGP neighbour transitions to the Established state.</li> <li>■ <b>bgpBackwardTransNotification</b> - A BGP FSM transitions from a higher state to a lower state</li> </ul> </li> </li></ul> |



| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <p>for the BGP neighbour.</p> <ul style="list-style-type: none"> <li>■ <code>bgpPrefixThresholdExceededNotification</code> - The prefix count exceeds the threshold limit configured for IPv4 or IPv6 peer.</li> <li>■ <code>bgpPrefixThresholdClearNotification</code> - The prefix count drops below the warning threshold configured for the IPv4 or IPv6 peer if it has exceeded the threshold before.</li> </ul> <ul style="list-style-type: none"> <li>• <b>isis</b> – Enables traps for IS-IS routing: <ul style="list-style-type: none"> <li>◦ <code>isisAdjacencyChange</code></li> <li>◦ <code>isisAreaMismatch</code></li> <li>◦ <code>isisAttemptToExceedMaxSequence</code></li> <li>◦ <code>isisAuthenticationFailure</code></li> <li>◦ <code>isisAuthenticationTypeFailure</code></li> <li>◦ <code>isisCorruptedLSPDetected</code></li> <li>◦ <code>isisDatabaseOverload</code></li> <li>◦ <code>isisIDLenMismatch</code></li> <li>◦ <code>isisLSPTooLargeToPropagate</code></li> <li>◦ <code>isisManualAddressDrops</code></li> <li>◦ <code>isisMaxAreaAddressesMismatch</code></li> <li>◦ <code>isisOriginatingLSPBufferSizeMismatch</code></li> <li>◦ <code>isisOwnLSPPurge</code></li> <li>◦ <code>isisProtocolsSupportedMismatch</code></li> <li>◦ <code>isisRejectedAdjacency</code></li> <li>◦ <code>isisSequenceNumberSkip</code></li> <li>◦ <code>isisVersionSkew</code></li> </ul> </li> <li>• <b>ospf</b> – Enables traps for OSPF routing:</li> </ul> |

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <ul style="list-style-type: none"> <li>◦ ospfIfAuthFailure</li> <li>◦ ospfIfConfigError</li> <li>◦ ospfIfRxBadPacket</li> <li>◦ ospfIfStateChange</li> <li>◦ ospfLsdbApproachingOverflow</li> <li>◦ ospfLsdbOverflow</li> <li>◦ ospfMaxAgeLsa</li> <li>◦ ospfNbrStateChange</li> <li>◦ ospfOriginateLsa</li> <li>◦ ospfTxRetransmit</li> <li>◦ ospfVirtIfAuthFailure</li> <li>◦ ospfVirtIfConfigError</li> <li>◦ ospfVirtIfRxBadPacket</li> <li>◦ ospfVirtIfStateChange</li> <li>◦ ospfVirtIfTxRetransmit</li> <li>◦ ospfVirtNbrStateChange</li> </ul>                                                                                                                                                                                            |
| <b>scaleout</b> | <p>Enables the Scaleout group traps:</p> <ul style="list-style-type: none"> <li>• <b>infrastructure</b> - Enables Infrastructure group traps: <ul style="list-style-type: none"> <li>◦ <b>all</b> – Enables all the infrastructure traps.</li> <li>◦ <b>cluster</b> – Enables cluster group traps. <ul style="list-style-type: none"> <li>■ <b>election</b> – Enables election status trap.</li> <li>■ <b>master-calling-re-election</b> – Enables re-election trap.</li> <li>■ <b>node-status</b> – Enables active node status trap.</li> </ul> </li> <li>◦ <b>master-node</b> – Enables master node group traps. <ul style="list-style-type: none"> <li>■ <b>traffic-map-distribution</b> – Enables Traffic-</li> </ul> </li> </ul> </li> </ul> |

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <p>map distribution trap.</p> <ul style="list-style-type: none"> <li>■ <code>vserver-traffic-map-update</code> – Enables vServer Traffic-map trap.</li> <li>○ <code>service-node</code> – Enables service node group traps.</li> <li>■ <code>local-device-disabled</code> – Enables local device disabled trap.</li> <li>■ <code>service-master</code> – Enables service-master trap.</li> <li>■ <code>traffic-map-update</code> – Enables traffic map update trap.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>slb</b> | <p>Enables the SLB group traps:</p> <ul style="list-style-type: none"> <li>• <code>application-buffer-limit</code> - Indicates that the configured SLB application buffer threshold has been exceeded.</li> <li>• <code>bw-rate-limit-exceed</code> – Indicates that the bw-rate-limit is exceeded by either a real server or a real port or both.</li> <li>• <code>bw-rate-limit-resume</code> – 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.</li> <li>• <code>gateway-down</code> – Enable gateway down trap only.</li> <li>• <code>gateway-up</code> – Enable gateway up trap only.</li> <li>• <code>server-conn-limit</code> - Indicates that an SLB server has reached its configured connection limit.</li> <li>• <code>server-conn-resume</code> – Indicates that an SLB server has reached its configured connection-resume value.</li> <li>• <code>server-disabled</code> – Indicates that an SLB server has been disabled.</li> <li>• <code>server-down</code> – Indicates that an SLB server has gone</li> </ul> |

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p>down.</p> <ul style="list-style-type: none"> <li>• <b>server-selection-failure</b> – Indicates that SLB was unable to select a real server for a request.</li> <li>• <b>server-up</b> – Indicates that an SLB server has come up.</li> <li>• <b>service-conn-limit</b> – Indicates that an SLB service has reached its configured connection limit.</li> <li>• <b>service-conn-resume</b> – Indicates that an SLB service has reached its configured connection-resume value.</li> <li>• <b>service-down</b> – Indicates that an SLB service has gone down.</li> <li>• <b>service-group-down</b> – Indicates that an SLB service group has gone down.</li> <li>• <b>service-group-member-down</b> – Indicates that an SLB service group member has gone down.</li> <li>• <b>service-group-member-up</b> – Indicates an SLB service group member has come up.</li> <li>• <b>service-group-up</b> – Indicates that an SLB service group has come up.</li> <li>• <b>service-up</b> – Indicates that an SLB service has come up.</li> </ul> |
| <b>slb</b><br>(cont.) | <ul style="list-style-type: none"> <li>• <b>vip-connnlimit</b> – Indicates that the connection limit configured on a virtual server has been exceeded.</li> <li>• <b>vip-connnratelimit</b> – Indicates that the connection rate limit configured on a virtual server has been exceeded.</li> <li>• <b>vip-down</b> – Indicates that an SLB virtual server has gone down.</li> <li>• <b>vip-port-connnlimit</b> – Indicates that the connection limit configured on a virtual port has been exceeded.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <ul style="list-style-type: none"> <li>• <b><code>vip-port-connratelimit</code></b> – Indicates that the connection rate limit configured on a virtual port has been exceeded.</li> <li>• <b><code>vip-port-down</code></b> – Indicates that an SLB virtual service port has gone down.</li> <li>• <b><code>vip-port-qps</code></b> – Indicates that the QPS value exceeds the configured high threshold, drops below the configured low threshold, or returns to a normal level.</li> <li>• <b><code>vip-port-up</code></b> – 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.</li> <li>• <b><code>vip-up</code></b> – Indicates that an SLB virtual server has come up.</li> </ul> |
| <b><code>slb-change</code></b> | <p>Enables the SLB change traps:</p> <ul style="list-style-type: none"> <li>• <b><code>connection-resource-event</code></b> - Enables system connection resource event trap.</li> <li>• <b><code>resource-usage-warning</code></b> – Indicates resource usage threshold met.</li> <li>• <b><code>server</code></b> – Indicates a real server was created or deleted.</li> <li>• <b><code>server-port</code></b> – Indicates a real server port was created or deleted.</li> <li>• <b><code>ssl-cert-change</code></b> – Indicates that an SSL certificate has been changed.</li> <li>• <b><code>ssl-cert-expire</code></b> – Indicates that an SSL certificate has expired.</li> <li>• <b><code>system-threshold</code></b> – Indicates that the device has</li> </ul>                                                                            |

| Parameter     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <p>exceeded the Usage threshold for a specified SLB resource.</p> <ul style="list-style-type: none"> <li>• <b>vip</b> – Indicates a virtual server was created or deleted.</li> <li>• <b>vip-port</b> – Indicates a virtual service port was created or deleted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>snmp</b>   | <p>Enables SNMP group traps:</p> <ul style="list-style-type: none"> <li>• <b>linkdown</b> – Indicates that an Ethernet interface has gone down.</li> <li>• <b>linkup</b> – Indicates that an Ethernet interface has come up.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>system</b> | <p>Enables the system group traps:</p> <ul style="list-style-type: none"> <li>• <b>all</b> - Enables all system group traps.</li> <li>• <b>apps-global</b> - Enables apps-global group traps. <ul style="list-style-type: none"> <li>◦ <b>cps-threshold</b> - Enables Connection per second (CPS) trap.</li> <li>◦ <b>sessions-threshold</b> - Enables number of sessions threshold trap.</li> </ul> </li> <li>• <b>control-cpu-high</b> – Indicates that the control CPU utilization is higher than the configured threshold.</li> <li>• <b>data-cpu-high</b> – Indicates that data CPU utilization is higher than the configured threshold.</li> <li>• <b>fan</b> – Indicates that a system fan has failed. Contact A10 Networks, Inc..</li> <li>• <b>file-sys-read-only</b> – Indicates that the file system has entered read-only mode.</li> <li>• <b>high-disk-use</b> – Enables system high disk usage traps.</li> </ul> |

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <ul style="list-style-type: none"> <li>• <b>high-memory-use</b> - Indicates that the memory usage on the ACOS Device is higher than the configured threshold.</li> <li>• <b>high-temp</b> - Indicates that the temperature inside the ACOS chassis is higher than the configured threshold.</li> <li>• <b>license-management</b> - Enables license management traps.</li> <li>• <b>low-temp</b> - Enables system low temperature trap.</li> <li>• <b>packet-drop</b> - Indicates that the number of dropped packets during the previous 10-second interval exceeded the configured threshold.</li> </ul> <p><b>NOTE:</b> This trap is not applicable to some device types. The trap is applicable to Thunder Series and AX Series hardware-based models and software-based models.</p> <ul style="list-style-type: none"> <li>• <b>power</b> - Indicates that a power supply has failed. Contact A10 Networks, Inc..</li> <li>• <b>pri-disk</b> - 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 chassis.</li> <li>• <b>restart</b> - Indicates that the ACOS Device is going to reboot or reload.</li> <li>• <b>sec-disk</b> - 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 chassis.</li> </ul> |

| Parameter               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | <p><b>NOTE:</b> This trap applies only to models that use disk drives.</p> <ul style="list-style-type: none"> <li>• <b>shutdown</b> – Indicates that the ACOS Device has shut down.</li> <li>• <b>smp-resource-event</b> – Enables system smp resource event trap.</li> <li>• <b>start</b> – Indicates that the ACOS Device has started.</li> <li>• <b>syslog-severity-one</b> - Enables system syslog severity one message trap.</li> <li>• <b>tacacs-server-up-down</b> - Enables system TACACS monitor server is up or down trap.</li> </ul> |
| <b>vcs state-change</b> | Enable the VCS state-change trap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>vrrp-a</b>           | <p>Enables VRRP-A high availability traps:</p> <p><b>active</b> - Indicates a device has become the active device.</p> <p><b>standby</b> - Indicated a device has become the standby device.</p>                                                                                                                                                                                                                                                                                                                                                |

**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, 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).<br>REQUIRED.<br>Alphanumeric |
|            | OPTIONAL.<br>Alphabetic.<br>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                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>group-name</i>     | Specifies the name of the SNMP group.                                                                                                                    |
| auth                  | Uses packet authentication but does not encrypt the packets.<br><br>(This is the authNoPriv security level.)                                             |
| noauth                | Does not use any authentication of packets.<br><br>(This is the noAuthNoPriv security level.)                                                            |
| priv                  | Uses packet authentication and encryption.<br><br>(This is the authPriv security level.)                                                                 |
| read <i>view-name</i> | Specifies the name of a read-only view for accessing the MIB object values.<br><br>Views are created using the <a href="#">snmp-server view</a> 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                                                                      |
|------------------------------------|----------------------------------------------------------------------------------|
| <i>trap-receiver</i>               | Hostname or IP address of the remote device to which traps will be sent.         |
| <i>version</i> {v1   v2c   v3}     | SNMP version. If you omit this option, the trap receiver can use SNMP v1 or v2c. |
| <i>community-string</i>            | Community string for the v1 or v2c traps.                                        |
| <i>user name</i>                   | SNMP v3 user name for sending the traps.                                         |
| <i>udp-port</i><br><i>port-num</i> | 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<br>read { <i>string</i><br>  encrypted}                                                                             | Define a community string with the following options: <ul style="list-style-type: none"> <li><i>string</i> - Define the value of the community string.</li> <li>encrypted - Define the community string with an encrypted password. Do NOT use this option manually.</li> </ul> |
| oid <i>oid-value</i>                                                                                                          | Object ID.<br><br>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 {<br><i>ipv4addr</i><br>[/ <i>mask-length</i>  <br><i>mask</i> ]  <br><i>ipv6addr</i>  <br><i>DNS-remote-host</i><br>} | Restricts SNMP access to a specific remote host or subnet.<br><br>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 and AX 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
<i>username</i>	Specifies the SNMP user name.
<i>groupname</i>	Specifies the group to which the SNMP user belongs.
<i>v3</i>	Specifies SNMP version 3.
<code>{auth {md5 sha sha-512 sha-384 sha-256 sha-224} {string encrypted}}</code>	Specifies the encryption method to use for user authentication. • <i>md5</i> - Uses Message Digest Algorithm 5 (MD5) for authentication. • <i>sha</i> - Uses Security Hash Algorithm (SHA) for authentication. • <i>sha-512</i> - Uses SHA with key size of 512 bits for authentication. • <i>sha-384</i> - Uses SHA with key size of 384 bits for authentication. • <i>sha-256</i> - Uses SHA with key size of 256 bits for authentication. • <i>sha-224</i> - Uses SHA with key size of 224 bits for authentication. • The sub-options for authentication are as follows: • <i>string</i> - Define the value of the community string. • <i>encrypted</i> - Define the community string with an encrypted password. Do NOT use this option manually.
<i>auth-password</i>	Password for user authentication.
<code>priv {des aes aes-192 aes-256}</code>	Specifies the encryption method to use for user privacy. • <i>aes</i> - Uses Advanced Encryption Standard (AES) algorithm. This uses a

Parameter	Description
	fixed block size of 128 bits. AES encryption supersedes DES encryption. • <code>aes-192</code> - Uses AES algorithm with key size of 192 bits for encryption. • <code>aes-256</code> - Uses AES algorithm with key size of 256 bits for encryption. • <code>des</code> - Uses Data Encryption Standard (DES) algorithm to apply a 56-bit key to each 64-bit block of data. This is considered strong encryption.
<code>priv-password</code>	Password for message encryption and privacy (8-31 characters).
<code>noauth</code>	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
<code>[tablename oid]</code>	Specifies the table name or OID. You can specify a string of 1-128 characters.
<code>timeout value</code>	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
<i>view-name</i>	Name of the SNMP view.
<i>oid</i>	MIB family name or OID.
<i>oid-mask</i>	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
<code>all</code>	All packets.
<code>so_pkts_conn_in</code>	Total packets processed for an established connection.
<code>so_pkts_conn_redirect</code>	Total packets redirected for an established connection.
<code>so_pkts_dropped</code>	Total packets dropped.
<code>so_pkts_errors</code>	Total packet errors.
<code>so_pkts_in</code>	Total number of incoming packets.
<code>so_pkts_new_conn_in</code>	Total packets processed for a new connection.
<code>so_pkts_new_conn_redirect</code>	Total packets redirected for a new connection.
<code>so_pkts_out</code>	Total number of packets sent out.
<code>so_pkts_redirect</code>	Total number of packets redirected.
<code>so_pkts_conn_sync_fail</code>	Total number of connection sync failures.
<code>so_pkts_nat_reserve_fail</code>	Total number of NAT reserve failures.
<code>so_pkts_nat_release_fai</code>	Total number of NAT release failures.
<code>so_pkts_conn_l7_sync</code>	Total number of Layer 7 connection syncs.
<code>so_pkts_conn_l4_sync</code>	Total number of Layer 4 connection syncs.
<code>so_pkts_conn_nat_sync</code>	Total number of NAT connection syncs.
<code>so_pkts_redirect_conn_aged_out</code>	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
<i>seconds</i>	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.

ssh

Description Perform an SSHD operation on the system.

Syntax

```

ssh
{
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 <i>url</i> 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: • <i>tftp://host/file</i> • <i>ftp://[user@]host[port:]/file</i> • <i>scp://[user@]host/file</i>

Parameter	Description
	<code>sftp://[user@]host/file</code>
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 <i>num</i>	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
<i>num</i>	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.
<i>num</i>	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 <i>num</i>	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 <i>seconds</i>	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 <i>num</i>	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 <i>num</i>	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.

NOTE: The AX 5200-11 requires 96 Gb of memory to support this feature. To check that your system meets this requirement, use the `show memory system` CLI command.

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 an AX 5630:

```
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
<code>delete-referenced-tagged-objects</code>	Enables the deletion of SLB objects that are tagged and referenced elsewhere in the system. When this command is enabled, the system allows

Parameter	Description
enable	the deletion of SLB objects even if they are referenced by other configurations or objects within the system.
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 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
<code>pu-sync-detection</code>	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
<code>enable</code>	Enables the detection of configuration synchronization between PU1 and PU2.
<code>disable</code>	Disables the detection of configuration synchronization between PU1 and PU2.
<code>interval</code>	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 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 NVIDIA 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 <i>percent</i>	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 <i>percent</i>	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 <i>tcp</i>	Disallows the creation of new TCP sessions.
disallow-new-sessions <i>udp</i>	Disallows the creation of new UDP sessions.
packets-	Maximum number of packets per second any CPU can

Parameter	Description
<code>per-second</code> <code>min num-</code> <code>pkts</code>	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 system.

Option	Description
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 retransmitted.
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_ssl_succ	Total number of SSL client-side sessions that connected successfully.

Option	Description
<code>slb_dns_server_ssl_succ</code>	Total number of SSL server-side sessions that connected successfully.
<code>slb_dns_udp_conn</code>	Total number of backend UDP connections.
<code>slb_dns_udp_conn_succ</code>	Total number of backend UDP connections that were established.
<code>slb_dns_padding_to_server_removed</code>	Total number of EDNS(0) padding to the server that were removed.
<code>slb_dns_padding_to_client_added</code>	Total number of EDNS(0) padding to client there were added (if client SSL is configured).
<code>slb_dns_edns_subnet_to_server_removed</code>	Total number of EDNS(0) client subnet from client queries that were removed.
<code>slb_dns_udp_retransmit</code>	Total number of SLB DNS UDP that were retransmitted.
<code>slb_dns_udp_retransmit_fail</code>	Total number of SLB DNS UDP that were retransmitted, but failed.
<code>rpz_action_drop</code>	Total number of actions dropped for RPZ (Response Policy Zone).
<code>rpz_action_pass_thru</code>	Total number of pass through actions for RPZ (Response Policy Zone).
<code>rpz_action_tcp_only</code>	Total number of TCP only actions for RPZ (Response Policy Zone).
<code>rpz_action_nxdomain</code>	Total number of NXDOMAIN actions for RPZ (Response Policy Zone).
<code>rpz_action_nodata</code>	Total number of NODATA actions for RPZ (Response Policy Zone).
<code>rpz_action_local_data</code>	Total number of Local Data actions for RPZ (Response Policy Zone).

Option	Description
<code>slb_drop</code>	Total number of DNS requests dropped.
<code>nat_slb_drop</code>	Total number of NAT DNS requests dropped.
<code>invalid_q_len_to_udp</code>	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-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 Load or unload 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	Unload 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	Load 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 GeoLite2-Country database which is available from http://www.maxmind.com • iana - Load built-in IANA database. • <i>name</i> - 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 Chassis Platforms (like TH7650 and TH14045). The databases do not synchronize with both PUs after being loaded.

Example

```
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
<i>num</i>	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 is available only on TH14045, TH7655 (Lite), and TH6435 devices.

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
<i>monitor_</i>	Specify the health monitor object name.

Parameter	Description
<i>name</i>	
<code>l2-bfd</code>	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.
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

Option	Description
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
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
<code>all</code>	All packets
<code>over_limit_drop</code>	Over limit drops
<code>limit_intf_drop</code>	Interfaces rate limit drops
<code>limit_vserver_drop</code>	Virtual Server rate limit drops
<code>limit_total_drop</code>	Total rate limit drops
<code>lockup_time_left</code>	Lockup time left
<code>curr_rate</code>	Current rate
<code>v6_over_limit_drop</code>	Over limit drops (v6)
<code>v6_limit_intf_drop</code>	Interfaces rate limit drops (v6)
<code>v6_limit_vserver_drop</code>	Virtual Server rate limit drops (v6)
<code>v6_limit_total_drop</code>	Total rate limit drops (v6)
<code>v6_lockup_time_left</code>	
<code>v6_curr_rate</code>	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
<code>all</code>	all
<code>in_msg</code>	In Messages
<code>in_errors</code>	In Errors
<code>in_dest_un_reach</code>	In Destination Unreachable
<code>in_pkt_too_big</code>	In Packet too big
<code>in_time_exceeds</code>	In TTL Exceeds
<code>in_parm_prob</code>	In Parameter Problem
<code>in_echos</code>	In Echo requests
<code>in_echo_reply</code>	In Echo replies
<code>in_grp_mem_query</code>	In Group member query
<code>in_grp_mem_resp</code>	In Group member reply
<code>in_grp_mem_reduction</code>	In Group member reduction
<code>in_router_sol</code>	In Router solicitation
<code>in_ra</code>	In Router advertisement
<code>in_ns</code>	In neighbor solicitation
<code>in_na</code>	In neighbor advertisement
<code>in_redirect</code>	In Redirects
<code>out_msg</code>	Out Message
<code>out_dst_un_reach</code>	Out Destination Unreachable
<code>out_pkt_too_big</code>	Out Packet too big
<code>out_time_exceeds</code>	Out TTL Exceed
<code>out_param_prob</code>	Out Parameter Problem
<code>out_echo_req</code>	Out Echo requests
<code>out_echo_replies</code>	Out Echo replies
<code>out_rs</code>	Out Router solicitation
<code>out_ra</code>	Out Router advertisement
<code>out_ns</code>	Out neighbor solicitation

Option	Description
<code>out_na</code>	Out neighbor advertisement
<code>out_redirects</code>	Out Redirects
<code>out_mem_resp</code>	Out Group member reply
<code>out_mem_reductions</code>	Out Group member reduction
<code>err_rs</code>	Error Router solicitation
<code>err_ra</code>	Error Router advertisement
<code>err_ns</code>	Error Neighbor solicitation
<code>err_na</code>	Error Neighbor advertisement
<code>err_redirects</code>	Error Redirects
<code>err_echoes</code>	Error Echo requests
<code>err_echo_replies</code>	Error Echo replies

Mode Configuration mode

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
<code>crypto-core <i>num</i></code>	Assign the number of crypto cores for processing IPsec packets. The value can be between 0 to 64.
<code>crypto-mem <i>percentage</i></code>	Assign the percentage of crypto memory for processing IPsec packets (rounded to increments of 10). The value can be between 0 to 100.
<code>fpga-decrypt</code>	Enable or disable the FPGA decryption offload.

Parameter	Description
{enable disable}	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 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
<code>ipv4-dest-list</code>	Specify this option to create an IPv4 Destination Threat List. It is a class list of IPv4 destination addresses.
<code>ipv4-source-list</code>	Specify this option to create an IPv4 Source Threat List. It is a class list of IPv4 source addresses.
<code>ipv6-dest-list</code>	Specify this option to create an IPv6 Destination Threat List. It is a class list of IPv6 destination addresses.
<code>ipv6-source-list</code>	Specify this option to create an IPv6 Source Threat List. It is a class list of IPv6 source addresses.
<code>ipv4-internet-host-list</code>	Specify this option to create an IPv4 Internet Host Threat List. It is a class list of IPv4 internet-hosts/subscriber addresses.
<code>ipv6-internet-host-list</code>	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 <i>list-name</i> [ip-threat-action <i>template_num</i>]	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 <i>template_num</i> option.
white-list <i>list-name</i>	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 from 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 ipv6-prefix-length

Description Configures the length of the source and the destination IPv6 prefix.

- For Dual-blade chassis platform, 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
<i>length</i>	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-to-IPv6 Transition Solutions Guide*.

Example

The following is the configuration example for IPv6 prefix length in chassis platform:

```
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 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 <i>num</i>	Configure a monitor template. Replace <i>num</i> with 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 <i>options</i>	Specifies the action to perform when a monitored event is detected. • clear sessions{ all sequence <i>num</i> } {all-partitions partition <i>name</i>} - Clear sessions • link-disable eth <i>portnum</i> sequence <i>num</i> - Specify the interfaces to be disabled • link-enable eth <i>portnum</i> sequence <i>num</i>

Command	Description
	- Specify the interfaces to be enabled
<code>[no] monitor</code> <i>options</i>	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. • <code>link-down eth portnum [eth portnum ...]</code> <code>sequence order</code> - Specify the interfaces to be monitored for link-down event • <code>link-up eth portnum [eth portnum ...]</code> <code>sequence order</code> - Specify the interfaces to be monitored for link-up event
<code>[no] monitor-and</code>	Uses the logical operator “AND” for link monitoring. The actions are performed only if <i>all</i> of the monitored events are detected. This is selected by default.
<code>[no] monitor-or</code>	Uses the logical operator “OR”. The actions are performed if <i>any</i> 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
<code>all</code>	All
<code>good_recv</code>	Good Router Solicitations (R.S.) Received
<code>periodic_sent</code>	Periodic Router Advertisements (R.A.) Sent
<code>rate_limit</code>	R.S. Rate Limited
<code>bad_hop_limit</code>	R.S. Bad Hop Limit

Option	Description
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
<i>path-object</i>	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: <i>ethernet <portnum></i>- Specify the two ethernet data ports. <i>trunk <trunknum></i>- Specify the two trunk interface.
use <i>monitor_name</i>	Specify the name of the health monitor that is defined under system health-check .

Parameter	Description
user-tag <i>user_ tag_name</i>	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
<i>policy_level</i>	Specifies the password complexity. The options are as follows: • Strict • Medium • Default • Simple
aging <i>val</i>	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 <i>val</i>	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

Parameter	Description
	passwords
min-pswd-len <i>num</i>	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 user-name check.
repeat-character-check [enable disable]	Enables or disables password repeat character check.
forbid-consecutive-character <i>num</i>	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.
<i>limit</i>	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	<code>ACOS(config)# system prio-queue-support enable</code>
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	<code>[no] system promiscuous-mode</code>
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	<code>[no] system q-in-q</code> This command enters the Q-in-Q Configuration mode where the following commands are available:

Parameter	Description
inner-tpid <i>num</i>	Set the Tag Protocol Identifier (TPID) of the inner VLAN tags to <i>num</i> .
outer-tpid <i>num</i>	Set the Tag Protocol Identifier (TPID) of the outer VLAN tags to <i>num</i> .
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 `cgnav6 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
<code>[no] accounting</code>	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 <code>delete-entry-and-sessions</code> command is applicable for CGN sessions only.
[no] attribute <i>attr-name</i> [[vendor <i>vendor-id</i>] number <i>attr-id</i>]	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 <i>num</i> – Charging Gateway Address. • sgsn-address <i>num</i> – Serving GPRS Support Node Address. • ggsn-address <i>num</i> – Gateway GPRS Support Node Address. • rat-type <i>num</i> – Radio Access Technology type. • user-location <i>num</i> - User location. • inside-ipv6-prefix prefix-length <i>num</i> – 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 <i>vendor-id</i> specifies the RADIUS vendor ID and can be 1-65535. The <i>attr-id</i> 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 MSISDN, or IMEI, and so on. For example, if your RADIUS server normally sends the MSISDN attribute as attribute 31, you could use the following command to configure the ACOS device to use the same attribute value for MSISDN: <pre>attribute msisdn number 31</pre>
[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: <pre>ip-list - IP list of remote clients.</pre>
[no] secret { name encrypted }	Specifies the password string used to authenticate RADIUS traffic.

Command	Description
<code>[no] vrid num</code>	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
<i>name</i>	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 <i>num</i> - Number of cache-template limits allowed • client-ssl-template-cfg <i>num</i> - Number of client-ssl-template limits allowed • conn-reuse-template-cfg <i>num</i> - Number of conn-reuse-template limits • fast-tcp-template-cfg <i>num</i> - Number of fast-tcp-template limits • fast-udp-template-cfg <i>num</i> - Number of fast-udp-template limits allowed • fix-template-cfg <i>num</i> - Number of fix-template limits allowed • http-template-cfg <i>num</i> - Number of http-template limits allowed • link-cost-template-cfg <i>num</i> - Number of link-cost-template limits • persist-cookie-template-cfg <i>num</i> - Number of persist-cookie-template limits allowed • persist-srcip-template-cfg <i>num</i> - Number of persist-srcip-template limits allowed • proxy-template-cfg <i>num</i> - Number of proxy-template limits allowed • server-ssl-template-cfg <i>num</i> - Number of server-ssl-template limits allowed

¹GSLB parameters are configurable on a per-partition basis hard-coded (and thus non-configurable) at the system level.

Parameter	Description
	• stream-template-cfg <i>num</i> - Number of stream-template limits allowed • gslb-device-cfg max <i>num</i> - Number of GSLB devices allowed • gslb-geo-location-cfg max <i>num</i> - Number of GSLB geo-locations allowed • gslb-ip-list-cfg max <i>num</i> - Number of GSLB IP lists allowed • gslb-policy-cfg max <i>num</i> - Number of GSLB policies allowed • gslb-service-cfg max <i>num</i> - Number of GSLB services allowed • gslb-service-ip-cfg max <i>num</i> - Number of GSLB service IPs allowed • gslb-service-port-cfg max <i>num</i> - Number of GSLB service-ports allowed • gslb-site-cfg max <i>num</i> - Number of GSLB sites allowed • gslb-svc-group-cfg max <i>num</i> - Number of GSLB service group allowed • gslb-template-cfg max <i>num</i> - Number of GSLB templates allowed • gslb-zone-cfg max <i>num</i> - Number of GSLB zones allowed • health-monitor-cfg max <i>num</i> - Number of health monitor checks a server uses • real-port-cfg max <i>num</i> - Number of real ports allowed. • real-server-cfg max <i>num</i> - Number of real servers allowed • service-group-cfg max <i>num</i> - Number of service groups allowed

Parameter	Description
	• threshold <i>percent</i> – 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 <i>num</i> – 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 <i>num</i> – Number of lines allowed in an IPv4 ACL • ipv6-acl-line-cfg max <i>num</i> - Number of lines allowed in an IPv6 ACL • object-group-cfg max <i>num</i> - Number of object group clauses allowed • object-group-clause-cfg max <i>num</i> - Number of object groups allowed • static-arp-cfg <i>num</i> – Number of static IPv4 ARPs or IPv6 neighbors allowed • static-ipv4-route-cfg <i>num</i> – Number of static IPv4 routes allowed • static-ipv6-route-cfg <i>num</i> – Number of static IPv6 routes allowed • static-mac-cfg <i>num</i> – Number of static MAC addresses allowed • static-neighbor-cfg <i>num</i> – Number of static neighbors allowed • threshold <i>percent</i> – 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 <i>percent</i> – 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
<i>resource-type</i>	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 <i>num</i> - Maximum file size allowed for AAM HTML files (default 20 Kbytes). • auth-session-count <i>num</i> - Total auth sessions in the system. • auth-portal-image-file-size <i>num</i> - 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<i>num</i> - 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. • max-aflex-authz-collection-number - Maximum number of collections supported by aFlex authorization. • l4-session-count <i>num</i> - 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.

Command	Description
	NOTE: The show system-resource usage command displays the cumulative L4 session count in a multi-PU system. • max-aflex-file-size <i>num</i> – Maximum size of an aFlex script in Kbytes. The default maximum allowable file size is 32K. • nat-pool-addr-count <i>num</i> – Total number of NAT pool addresses available for configuration in the system. The range is platform specific. • radius-table-size – Total number of configurable CGNV6 RADIUS table entries. • ram-cache-memory-limit <i>num</i> – 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 <i>num</i> – Maximum number of monitored entities for visibility. The specified number must be between 3840 and 162816 (inclusive). • nat-pool-addr-count <i>num</i> – Total number of NAT pool addresses available for configuration in the system. The range is platform specific. • waf-template-count <i>num</i> – Total number of WAF templates available for configuration in the system. The default value is 128. The minimum and maximum configurable values are platform specific.

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.

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
<code>age-timeout</code>	Specify the aging timeout for the server certificate status cache. (1-86400 seconds)
<code>max-cache</code>	Specify the maximum number of server certificate status cache. (1-2400)
<code>clear</code>	To clear or reset functions.
<code>do</code>	To run exec commands in config mode.
<code>end</code>	To end the configure mode.
<code>exit</code>	To exit from configure mode or sub mode.
<code>no</code>	To negate the command or set its defaults.
<code>show</code>	To show the running system information.
<code>write</code>	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-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
<code>ipv4-only</code>	Enable IPv4 hardware forward entries only.
<code>ipv6-only</code>	Enable IPv6 hardware forward entries only.
<code>ipv4-ipv6</code>	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 baselining 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
<code>audit enable auto-sync disable</code>	Enables the integrity check and disables the auto-sync.
<code>audit disable</code>	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
<code>activeopens</code>	Active open conns
<code>passiveopens</code>	Passive open conns
<code>attemptfails</code>	
<code>estabresets</code>	Resets rcvd on EST conn
<code>insegs</code>	Total in TCP packets
<code>outsegs</code>	Total out TCP packets
<code>retranssegs</code>	Retransmitted packets
<code>inerrs</code>	Input errors
<code>outrsts</code>	Reset Sent
<code>sock_alloc</code>	Sockets allocated
<code>orphan_count</code>	Orphan sockets
<code>mem_alloc</code>	Memory alloc
<code>recv_mem</code>	Total rx buffer
<code>send_mem</code>	Total tx buffer
<code>currestab</code>	Currently EST conns
<code>currsysnt</code>	TCP in SYN-SNT state
<code>currsynrcv</code>	TCP in SYN-RCV state
<code>currfinw1</code>	TCP in FIN-W1 state
<code>currfinw2</code>	TCP FIN-W2 state
<code>currtimew</code>	TCP TimeW state

Parameter	Description
<code>currclose</code>	TCP in Close state
<code>currc1sw</code>	TCP in CloseW state
<code>currlack</code>	TCP in LastACK state
<code>currlstn</code>	TCP in Listen state
<code>currclsg</code>	TCP in Closing state
<code>pawsactiverejected</code>	TCP paw active rej
<code>syn_rcv_rstack</code>	Rcv RST ACK on SYN
<code>syn_rcv_rst</code>	Rcv RST on SYN
<code>syn_rcv_ack</code>	Rcv ACK on SYN
<code>ax_rexmit_syn</code>	TCP rexmit SYN
<code>tcpabortontimeout</code>	TCP abort on timeout
<code>noroute</code>	TCPIP out noroute
<code>exceedmss</code>	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
<code>rate-limit-reset-unknown-conn</code>	Configure rate limit for tcp reset-on-error.
<code>pkt-rate</code>	Packet rate.
<code>num</code>	Maximum rate to send out RESET per second (1-1048575).
<code>log</code>	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
<i>template-name</i>	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
<i>template-ID</i>	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).
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-13 | use-14}
```

Parameter	Description
use-13	Perform load balancing based on Layer 3 (IPv4 or IPv6) parameters.
use-14	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-13` or `use-14` 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-14` 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-13
```

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 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-robin	In the shared partition, this option assigns MAC 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.

Parameter	Description
	- 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 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](#)

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

Parameter	Description
	Filtering Policy. • general-policy <i><name></i> – Configures GTP General Policy. • logging-policy <i><name></i> – Configures GTP Logging Policy. • message-filtering-policy <i><name></i> interface-type {roaming non-roaming} – Configures GTP Message Filtering Policy. • msisdn-list <i><name></i> {permit deny} – Configures GTP MSISDN list. • rate-limit-policy <i><name></i> {monitor drop} – Configures GTP Rate Limit policy. • validation-policy <i><name></i> – Configures GTP Validation Policy. Specify the name (1-63 characters).
gtp-policy <i><name></i>	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-policy <i><num></i>	Creates a Limit policy. Specify the limit policy number (1 to 1023).
sctp { default <i><name></i> }	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
<i>template_num</i>	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
<code>idle-timeout <i>num</i></code>	Configure the idle timeout in minutes. You can specify a value from 1 to 1440. The default value is 5 minutes.
<code>log { enable disable }</code>	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]
```

Parameter	Description
<i>hostname</i>	Host name of the TACACS+ server. If a host name is used, make sure a DNS server has been configured.
<i>ipaddr</i>	IPv4 or IPv6 address of the TACACS+ server.
<i>secret</i> <i>secret-string</i>	Password, 1-127 characters, required by the TACACS+ server for authentication requests.
<i>port</i> <i>portnum</i>	The port used for setting up a connection with a TACACS+ server. The default port is 49.
<i>timeout</i> <i>seconds</i>	The maximum number of seconds allowed for setting up a connection with a TACACS+ server. The default timeout is 12 seconds.
<i>source</i>	The following options are available as the source

Parameter	Description
	secret properties: • <code>ethernet</code> - the source Ethernet interface ID port number • <code>ip</code> - the source IPv4 address string • <code>ipv6</code> - the source IPv6 address string • <code>lif</code> - the source logical interface ID number • <code>loopback</code> - the source loopback interface ID port number • <code>trunk</code> - the source trunk interface ID number • <code>ve</code> - the source Virtual Ethernet interface ID number

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":

```
ACOS(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:

```
ACOS(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":

```
ACOS(config)# no tacacs-server host 192.168.3.45
```

Example The following command deletes all TACACS+ servers:

```
ACOS(config) # no tacacs-server
```

tacacs-server monitor

Description Check the status of TACACS+ servers.

Syntax `[no] tacacs-server monitor [interval seconds]`

Parameter	Description
<i>seconds</i>	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-FPGA platform. (Only works for platform with 32GB disk size where the techreport retention period is set to 7 by default).
hang-recover-time <i>minutes</i>	Specify the device recovery time (in minutes) if the show techsupport command hangs. You can specify 15-1000 minutes.
interval <i>minutes</i>	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	Specify the maximum size (in gigabyte) of each techsupport log file that is saved on a regular basis

Parameter	Description
<i>gb</i>	(for a given day in a single file). You can specify 1-10 GB. The default size is 1 GB.
max-partitions <i>num</i>	Specify the maximum partitions to be displayed in each techsupport log file. You can specify 1-120. The default value is 30.
priority-partition <i>name</i>	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 the [show 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, 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.
gslb-prompt <i>options</i>	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 <i>number</i>]	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 <i>minutes</i>	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	Specifies the number of lines to display per page, 0-

Parameter	Description
<i>number</i>	512. To disable paging, enter 0. The default length is 24 lines.
prompt <i>hostname</i>	Display hostname in prompt.
width <i>lines</i>	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 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:

$1K\text{-blocksize} = 64MB\text{-filesize}$

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, 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
<i>zone</i>	Specify the time zone. Enter <code>timezone ?</code> at the CLI prompt to see a list of available time zones.
<code>nodst</code>	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 <i>image-name</i>	Delete any one existing local GUI image.
local <i>image-name</i>	Specify the upgrade image filename from the local image repository. Use <code>show gui-image-list</code> to view a list of available local images. The <i>image-name</i> can be 1-128 characters.
rollback <i>image-name</i>	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 <i>url</i>	Save the GUI image on the remote server using the specified url .
show-percentage <i>url</i>	Enable this option to view the file transmit percentage for the specified url .
source-ip-address <i>ip address</i> [save-gui <i>url</i> show-percentage <i>url</i> upload <i>url</i> <i>url</i>]	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:

Parameter	Description
	• save-gui url • show-percentage url • upload url • url
upload <i>url</i>	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 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 <i>url</i> show-percentage <i>url</i> upload <i>url</i> <i>url</i>] 	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

Parameter	Description
	url
<i>url</i>	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: <code>tftp://host/file</code> <code>ftp://[user@]host[:port]/file</code> <code>scp://[user@]host/file</code> <code>http://[user@]host/file</code> <code>https://[user@]host/file</code> <code>sftp://[user@]host/file</code> 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: <code>!#\$()*+,-.:/;<=>?@[\]</code> - The following special characters are not supported in the password: <code>(blank space) "%&'/:;<>?@[\]</code>

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 <i>image-name</i> [reboot-after-upgrade staggered-upgrade-mode Device <i>device-id</i>]	Specify the upgrade image from the local VCS image repository. Use show vcs images to view a list of available local images. The <i>image-name</i> can be 1-128 characters and the format should be: <i>aximage_XX_XX_XX_XX.tar.gz</i>. 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 <i>device-id</i> [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.

Parameter	Description
	The image will be rolled back to the most recent version that was previously saved on the Thunder device. In the following scenarios, the <code>rollback</code> command is unavailable: • Platforms with 32 GB or less disk size, such as TH840/TH940/TH1040. • The available disk size is less than 8GB.
<code>show-percentage url</code>	Enable this option to view the file transmit percentage for the specified url {reboot-after-upgrade staggered-upgrade-mode Device device-id [reboot-after-upgrade]}.
<code>source-ip-address ip address [show-percentage url]</code>	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]}
<code>use-mgmt-port [show-percentage url]</code>	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

Parameter	Description
	this command: • show-percentage url • url {reboot-after-upgrade staggered-upgrade-mode Device device-id [reboot-after-upgrade]}
<pre>url {reboot-after-upgrade staggered-upgrade-mode Device device-id [reboot-after-upgrade]}</pre>	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: • <code>tftp://host/file</code> • <code>ftp://[user@]host[:port]/file</code> • <code>scp://[user@]host/file</code> • <code>http://[user@]host/file</code> • <code>https://[user@]host/file</code> • <code>sftp://[user@]host/file</code> 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

Parameter	Description
	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 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 ACOS Virtual Chassis System (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	<code>[no] ve-stats enable</code>
Default	Disabled
Mode	Configuration mode
Usage	If the ACOS device is a member of an aVCS virtual chassis, use the <code>device-context</code> 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	<code>[no] vlan <i>vlan-id</i></code> Replace <i>vlan-id</i> with the ID of the VLAN (2-4094). If the ACOS device is a member of an aVCS virtual chassis, specify the <i>vlan-id</i> as follows: <i>DeviceID/vlan-id</i>
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: <pre>ACOS(config)# vlan 69 ACOS(config-vlan:69)#</pre>
Example	You cannot have duplicate VLANs configured across partitions. In this example, VLAN 10 is configured in the shared partition: <pre>ACOS(config)# vlan 10</pre>

```
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	<code>[no] vlan-global enable-def-vlan-l2-forwarding</code>
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	<code>[no] vlan-global 12-fwd-for-me-arp-ns</code>
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 12-fwd-for-me-arp-ns
```

vlan-global l3-vlan-fwd-disable

Description	Globally disable Layer 3 forwarding between VLANs.
Syntax	<code>[no] vlan-global l3-vlan-fwd-disable</code>
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 <code>l3-vlan-fwd-disable</code> action.

web-service

Description	Configures web services.
Syntax	<code>[no] web-service options</code>

Parameter	Description
<code>auto-redir</code>	Enables requests for the unsecured port (HTTP) to be automatically redirected to the secure port (HTTPS). This feature is enabled by default.
<code>axapi-session-limit</code> <i>num</i>	Specifies the maximum number of aXAPI sessions that can be run simultaneously (1-100). The default is 30.
<code>axapi-timeout-policy</code> <code>idle</code> <i>minutes</i>	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.
<code>axapi-token-sharing</code>	Enables sharing of aXAPI token within multiple hosts without the need to authenticate the hosts. This feature is disabled by default. NOTE: If <code>axapi-token-sharing</code> is enabled and multiple sessions are created, the outside hosts can access ACOS with the token from any session.
<code>gui-session-limit</code> <i>num</i>	Specifies the maximum number of GUI sessions that can be run simultaneously (1-100). The default is 30.
<code>gui-timeout-policy</code>	Specifies the number of minutes GUI session

Parameter	Description
idle <i>minutes</i>	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 <i>seconds</i>	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 <i>characters</i>	Specify the GUI login message (1-1985).
max-keep-alive-requests <i>num</i>	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 <i><num></i>	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 <i>num</i>	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 <i>num</i>	worker processes. A bigger number means more TCP connections can be established initially. The number should be less than the <code>mpm-max-conn</code> . Otherwise, the real value will be the same as <code>mpm-max-conn</code> .
port <i>port</i>	Specifies the port number for the unsecured (HTTP) port. The default HTTP port is 80.
pre-login-message <i>num</i>	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: ◦ <code>tftp://host/file</code> ◦ <code>ftp://[user@]host[port:]/file</code> ◦ <code>scp://[user@]host/file</code> ◦ <code>sftp://[user@]host/file</code> • 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 <i>port</i>	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 [<i>acl-id</i> <i>acl_name</i>] <i>binding</i>	Specify the IPv4 ACL by its ID or by its name. <i>binding</i> - Specify interfaces or ports associated with IPv4 ACLs.
ipv6 <i>acl_name</i>	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
<i>all-msgs</i>	Shows all logs in the system.
<i>message-id</i>	Shows all logs under the provided message-id as the following: <pre>acos-events message-id <message-id> all/node-only/children-only/log-field-only</pre> • <i>all</i> - Shows logs at this level and all sub-trees. • <i>node-only</i> - Shows logs at this node only. • <i>children-only</i> - Shows logs from all its sub-trees. • <i>log-field-only</i> - 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. • <i><message-id></i> 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.
<i>interface</i>	• <i>all</i> - Shows logs at this level and all sub-trees. • <i>node-only</i> - Shows logs at this node only. • <i>children-only</i> - Shows logs from all its sub-trees. • <i>log-field-only</i> - 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
<i>admin-name</i>	Administrator name.
<i>detail</i>	Shows detailed information about the admin account.
<i>session</i>	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 <i>Configuring Application Delivery Partitions</i> 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
<i>partition name</i>	Displays files only for a select partition.
<i>file-name</i>	Filters the show output for only files that partially match a specified <i>file-name</i> . 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
```

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
<i>partition name</i>	Displays files only for a select partition.
<i>filename</i>	Filters the show output for only files that partially match a specified filename. • <code>datacpu</code> - specify a data CPU to show • <code>format</code> - Specify which format to show: • <code>hex</code> HEX format • <code>hexl2</code> HEX format with I2 header • <code>hexascii</code> HEX & ASCII format

Parameter	Description
	• <code>hexasciil2</code> HEX & ASCII format with l2 header • <code>ascii</code> ASCII format • <code>l2</code> With l2 header • <code>verbose</code> Verbose • <code>verbose1</code> More verbose • <code>verbose2</code> More more verbose • <code>timeno</code> Without time • <code>timedelta</code> Show delta time • <code>timeformat</code> 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 23 22:49:07 2008	58801	Tue Sep
file123 26 17:06:51 2008	192	Fri Sep

```
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 disabled.
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 chassis platforms i.e. TH14045, TH7650. For Thunder 7650, the output is displayed only for one processing unit. For Thunder 14045 ACOS device, the output is displayed only for master.

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.

Field	Description
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.
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

Field	Description
	state can be one of the following: • Init • Up • AdminDown • 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.

Field	Description
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 sent....received	Statistics of control packets for this BFD 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.
Dcmmsg....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".

Field	Description
BFD Packet Multipoint is invalid	The value of the received multipoint flag is set to "1".
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	Number of times the destination IP address for a

Field	Description
Destination unreachable	BFD neighbor was unreachable while the ACOS was attempting to transmit a BFD packet to the neighbor.
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
```

NOTE: By default, data displayed for the “show bootimage” CLI output has been consolidated for chassis platforms i.e. TH14045, TH7650. For Thunder 7650, the output is displayed only for one processing unit. For Thunder 14045 ACOS device, the output is displayed only for Master.

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 bpdud-fwd-group

Description Display the configured Bridge Protocol Data Units (BPDU) forwarding groups.

Syntax `show bpdud-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 bpdud-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
<i>name</i>	Name of a black/white list.
detail	Displays the IP addresses contained in a black/white list.
<i>ipaddr</i>	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/bw1.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/bw1_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.
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”:

```
ACOS# 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 <i>num</i>	Display adjacency information for the specified ethernet interface.
lif <i>num</i>	Display adjacency information for the specified logical interface.
loopback <i>num</i>	Display adjacency information for the specified loopback interface.
management	Display adjacency information for the management interface.
trunk <i>num</i>	Display adjacency information for the specified trunk.
tunnel <i>num</i>	Display adjacency information for the specified tunnel.
ve <i>num</i>	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	<pre>show config</pre>
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	<pre>show config-block</pre>
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
<code>all-partitions</code>	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.
<code>detail</code>	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 <code>detail</code> 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 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#
```

NOTE: Data displayed for the “show core-slots” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650.

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
<code>show counters acos- events statistics</code>	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

Parameter	Description
	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. • 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 <code>show logs</code> and <code>show varlog</code>, 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
<code>show counters acos-events collector-group</code>	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 servers 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
<code>counters error</code>	Displays error counters
<code>counters error alert</code>	Display alert error counters.
<code>counters error critical</code>	Display critical error counters
<code>counters error warning</code>	Display warning error counters
<code>counters error out-of-res</code>	Display errors due to resource exhaustion
<code>counters drop</code>	Display drop counters
<code>counters drop alert</code>	Display alert drop counters
<code>counters drop critical</code>	Display critical drop counters
<code>counters drop warning</code>	Display warning drop counters
<code>counters drop out-of-res</code>	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: <i>Unable to create an entry in the IP threat list due to memory exhaustion</i>
Out of SPE Entries Error	Displays the following error: <i>Unable to add entries to SPE due to SPE resource limit or exhaustion</i>

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

Controll	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.

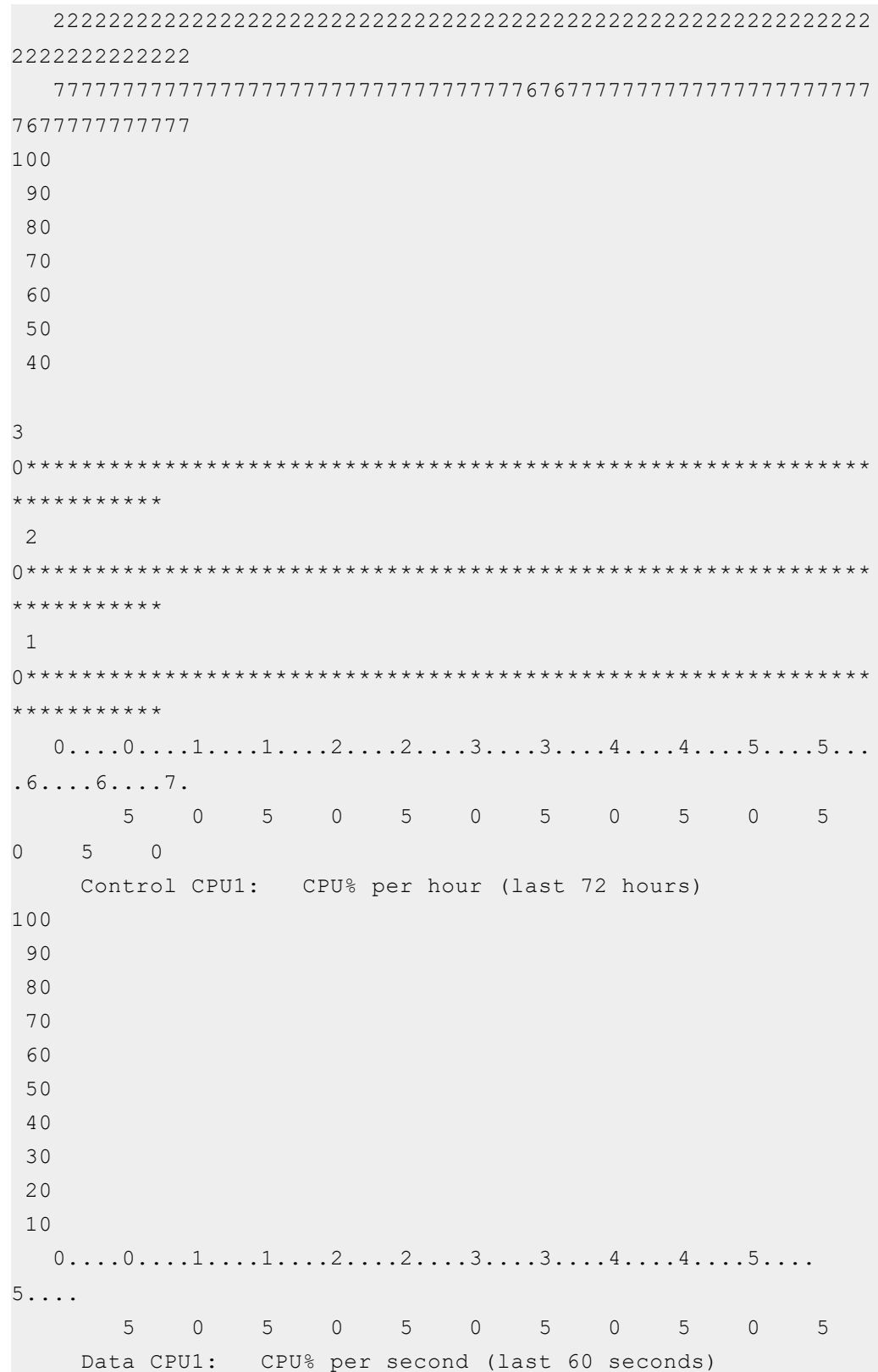
Field	Description
Time	System time when the statistics were gathered.
Control <i>n</i>	Control CPU.
Data <i>n</i>	Data CPU. The number of data CPUs depends on the ACOS model.
I/O <i>n</i>	IO CPU usage. I/O fields are displayed on non-FTA platforms only.
1Sec - 60sec	Time intervals at which statistics 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.

[illegible]

[illegible]



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
```

NOTE: Data displayed for the “show debug” CLI output has been consolidated for chassis platforms i.e. TH14045, TH7650. For Thunder 7650, the output is displayed only for one processing unit. For Thunder 14045 ACOS device, the output is displayed only for Master.

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 [all-entries | dns-class [string | <1-65535>] | dns-type
[string | <1-65535>] | domain-name [dns-domain-name | fqdn-
domain] name] | brief [max-rdata-size [<1-8192> | all] | max-
record-num [<1-1024> | all ] ] | detail [max-rdata-size [<1-
8192> | all] | max-record-num [<1-1024> | all ] ] ] |
global [all-entries | dns-class [string | <1-65535>] |
dns-type [string | <1-65535>] |
domain-name [dns-domain-name | fqdn-domain] name] |
brief [max-rdata-size [<1-8192> | all] | max-record-num [<1-
1024> | all ] ] | detail [max-rdata-size [<1-8192> | all] |
max-record-num [<1-1024> | all ] ] ] |
statistics
```

Parameter	Description
client	Display DNS client statistics.
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 <i>num</i> - Other class value (1-65535)

Parameter	Description
	• 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 ◦ <i>num</i> - Other type value (1-65535) • domain - You can specify either one of the following: ◦ dns-domain-name – Domain name ◦ fqdn-domain – Fully qualified domain name. • brief - Displays the DNS response resource records of the cache entry in brief. It displays only the answer 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 under options brief as well as detail: ◦ max-rdata-size - Specify the maximum rdata size for each record. Specify one of the following options:

Parameter	Description
	◦ <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 the number of maximum records to be displayed for each section of the cache entry. Specify one of the following options: ◦ <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 limit is 1024 records.
global	Display DNS cache global 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 query class ◦ ANY – ANY query class ◦ num - Other class value (1-65535)

Parameter	Description
	• 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 ◦ <i>num</i> - Other type value (1-65535) • domain-name - You can specify either one of the following: ◦ dns-domain-name – Domain name ◦ fqdn-domain – Fully qualified domain name. • brief - Displays the DNS response resource records of the cache entry in brief. It displays only the answer 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 under options brief as well as detail: ◦ max-rdata-size - Specify the maximum rdata size for each record. Specify one of the

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 DNS caching statistics:

```
ACOS#show dns cache statistics
Total allocated: 0
Total freed: 0
Total query: 0
Total server response: 0
Total cache hit: 0
Query not passed: 0
Response not passed: 0
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: 0
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: 0
Current data allocate: 0
```

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	Total number of DNS queries received by the ACOS.

Field	Description
Query	
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 answer records were available. NOTE: This behavior only applies to DNS “IN” class and “A” or “AAAA” types.
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.

Field	Description
Response With Multiple Questions	Number of responses that were not cached because they contained multiple question records. ACOS only supports one question record.
Response With Multiple Answers	Number of responses that were not cached because they contained more than one answer, when <code>single-answer</code> caching policy was enabled. NOTE: 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 <code>ttl-threshold</code> caching policy was enabled. NOTE: 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. NOTE: This feature is applicable only to VIP DNS Cache and requires the <code>dns-log-enable period</code> 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	Current allocated cache entries.

Field	Description
Allocate	
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.
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.
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.

Field	Description
No. of requests with no response	Number of DNS connection that did not received any response.
No. of request retransmits	Number of DNS connection receives retransmitted request from client.
No. of requests and responses not match	Number of DNS connection that receives 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.

Field	Description
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.
No. of request retransmits	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 sessions with clients.
No. of successful server tls	Number of successful DNS-over-TLS sessions 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 connections.
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 retransmission	Number of backend UDP retransmission in case of timeout.
No. of udp retransmission failed	Number of failed backend UDP retransmission.

Field	Description
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 client	Number of ECS data received from 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
<i>zone-name</i>	The name of the child zone. If you do not specify a zone name, DNSKEY resource records for all child zones are displayed.
partition <i>partition-name</i>	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
<i>zone-name</i>	The name of the child zone. If you do not specify a zone name, DS resource records for all child zones are displayed.
partition <i>partition-name</i>	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 <i>template-</i>	The name of the template. If you do not specify a template name, all DNSSEC templates are displayed.

Parameter	Description
<i>name</i>	
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#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

Parameter	Description
	• ipnat • 12-13-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
<code>partition-create</code>	View partition creation events.
<code>partition-delete</code>	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
<code>config</code>	Displays the fail-safe configuration entered by you or other admins.
<code>information</code>	Displays fail-safe settings and statistics. The output differs between models that use FPGAs 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 FPGAs 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 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 FPGA buffers the ACOS Device has. These buffers are allocated when the ACOS Device is booted. This number does not change during system operation. The FPGA device is logically divided into 2 domains,

Field	Description
	which each have their own buffers. The next two counters are for these logical FPGA domains.
Free FPGA Buffers in Domain 1	Number of FPGA buffers in Domain 1 that are currently free for new data.
Free FPGA Buffers in Domain 2	Number of FPGA buffers in Domain 2 that are currently free for new data.
Total Free FPGA Buffers	Total number of free FPGA buffers in both FPGA 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 FPGAs in hardware. (The FPGA 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	Total amount of the ACOS Device's memory that is allocated for session processing.

Field	Description
Memory	
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 FPGA 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 FPGA 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
<code>a10log</code>	Display information for logs present in the <code>a10log</code> directory. This directory contains showtech and support files.
<code>syslog</code>	Display information for logs present in the <code>syslog</code> directory. This directory contains Linux system logs.

Parameter	Description
varlog	Display information for logs present in the varlog directory. This directory contains ACOS system logs.
l	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 | bt dump.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
<i>num</i>	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
```

NOTE: Data displayed for the “show gui-image-list” CLI output has been consolidated for chassis platforms i.e. TH14045, TH7650. For Thunder 7650, the output is displayed only for one Processing Unit. For Thunder 14045 ACOS device, the output is displayed only for Master.

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
```

NOTE: Data displayed for the “show hardware” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650. It will contain doubled static values as total memory, CPUs, and storage.¹ But it will not contain dynamic per card information.

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

¹It displays the doubled static values for total memory, CPUs and storage respectively as mentioned below:

- a.Number of CPUs: If one processing unit has 48 cores, then it will show as 96.
- b.Total Storage Space: If one processing unit has 100G, then the total will be shown as 200G.
- c.Total Memory Space: If one processing unit has 250GB, then the total will be shown as 500G.

Parameter	Description
	monitoring.
monitor [<i>name</i>]	Shows configuration settings and status for the specified health monitor.
postfile [<i>name</i>]	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 17:         : 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

Field	Description
	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.
Timeout	Number of times a response was not received before the health check timed out.
Unexpected error	Number of unexpected errors that occurred.

Field	Description
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: $\text{total-monitors} / \text{global-timeout}$ 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.
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

Field	Description
	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 <i>Command Line Interface Reference for ADC</i> for Layer 3 health checks or “port” in the <i>Command Line Interface Reference for ADC</i> 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 (/). The number of times the most recent health check was retried before a response was received or the maximum number of retries was used.

Field	Description
	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 <code>up-retry</code> 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
```

```
total
```

```
-----
-----
```

```

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.
Smart NAT instance initialization error	Error initializing the Smart NAT instance.
Smart NAT SLB	Smart NAT failed to update the

Field	Description
server route update error	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 runs 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 runs 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 Address	Link	Dupl IPs	Speed Flags	Trunk Name	Vlan	Encap	MAC	IP

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						
lif_1	Up	N/A	N/A	N/A	1	N/A	5a1f.6334.0f6e	
0.0.0.0/0		0						
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 Address	Link	Dupl IPs	Speed Flags	Trunk Name	Vlan	Encap	MAC	IP

```

-----
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 Virtual Chassis System (VCS), this command provides device-specific media information.

On non-FPGA 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 <i>portnum</i>	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).

Parameter	Description
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	LocPrf	Weight	Next Hop	Type	Metric
*> 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 fragmentation or IPv4-in-IPv6 fragmentation or IPv6-in-IPv4 fragmentation.

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 <code>ipv6</code> option instead of the <code>ip</code> 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      100.100.100.1      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] |


```

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
<i>pool-name</i>	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
<code>statistics</code>	Displays statistics.
<code>ipaddr</code>	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, al0if0,
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
<i>list-name</i>	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 IPCMv6 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

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
```

```
al0-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      : CXXXXAAXXXX2C932C241F3C4B30FXXXXXXXXXXXXX
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
<code>debug</code>	Show debug logging entries only.
<code>length</code> <i>num</i>	Shows the most recent log entries, up to the number of entries you specify. You can specify 1-1000000 (one million) entries.
<code>policy</code>	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
<i>macaddr</i>	Shows the MAC table entry for the specified MAC address. Enter the MAC address in the following format: aaaa.bbbb.cccc
port <i>port-num</i>	Shows the MAC table entries for the specified Ethernet port.
vlan <i>vlan-id</i>	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 SNMP	SSH ACL	Telnet	HTTP	HTTPS
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	off
-							
eth2	on	off	off	off	off	off	off
-							
eth3	on	off	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  off  on  -
eth3      on   off  off  off  off  off  off  off -
eth4      on   off  off  off  off  off  off  on  -
eth5      on   off  off  off  off  off  off  on  -
eth6      on   off  off  off  off  off  off  on  -
ve110     on   off  off  off  off  off  off  on  -
ve210     on   off  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, 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
```

NOTE: Data displayed for the “show monitor” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650.

For Thunder 7650, the output is displayed only for one processing unit.

For Thunder 14045 ACOS device, the output is displayed only for master.

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.
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.

Field	Description
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.
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.
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. <i>cert-name</i> - Specifies a name for the certificate, and you can name with a maximum of 255 characters.

Option	Description
cert <i>cert-name</i>	Shows information about the certificates on the ACOS Device. To display information for a specific certificate, use the <i>cert-name</i> 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. <i>log</i> - Shows cmp-cert enrollment log and debug information. Use CMP certificate name. ACOS (config)# show pki cmp-cert log testingcert <i>status</i> - Shows CMP enrollment status. ACOS(config)#show pki cmp-cert status
scep-cert [log status]	Shows information about SCEP certificate. <i>log</i> - Shows scep-cert enrollment log and debug information. Use SCEP certificate name. <i>status</i> - Shows SCEP enrollment status. ACOS (config)# show pki scep-cert log testingcert
acme-cert [log status]	Shows information about ACME certificate. <i>log</i> - 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
	<i>status</i> - Shows ACME enrollment status. ACOS(config)#show pki acme-cert status
csr <i>csr-name</i>	Shows information about the certificate signing requests. To display information for a specific certificate signing request, use the <i>csr-name</i> 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: <u>partition {shared partition-name} is only supported in L3V partition.</u> <i>shared</i> - A specific partition. <i>partition-name</i> - You can display information from the shared partition or from a specific L3V partition. <i>sort-by</i> - 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
```

NOTE: Data displayed for the “show reboot” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650.
For Thunder 7650, the output is displayed only for one Processing Unit.
For Thunder 14045 ACOS device, the output is displayed only for Master.

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
<code>all-partitions</code>	Lists resource usage counters for all partitions.
<code>global</code>	Lists global resource usage counters.
<code>partition</code>	Lists resource usage counters for the specified

Parameter	Description
<code>{partition-name shared}</code>	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 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	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.

Field	Description
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  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
<i>file-num</i>	Log file number.
bgpd [<i>file-num</i>]	Displays the specified BGP log file, or all BGP log files.
isisd [<i>file-num</i>]	Displays the specified IS-IS log file, or all IS-IS log files.
nsm [<i>file-num</i>]	Displays the specified Network Services Module (NSM) log file, or all NSM log files.
ospf6d [<i>file-num</i>]	Displays the specified IPv6 OSPFv3 log file, or all OSPFv3 log files.
ospfd [<i>file-num</i>]	Displays the specified IPv4 OSPFv2 log file, or all OSPFv2 log files.
ripd [<i>file-num</i>]	Displays the specified IPv4 RIP log file, or all IPv4 RIP log files.
ripngd [<i>file-num</i>]	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
<i>filename</i>	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.al0networks.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 Display 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 a1013v1 id 1
!
hostname InsideAX
```


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# 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)#sh 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
!

```

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 <i>string</i> - 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 <i>num</i>—View sessions with the specified destination port (1-65535).

Parameter	Description
	• dest-v4-addr <i>ipaddr[/length]</i>—View sessions with the specified destination IPv4 address. • dest-v6-addr <i>ipaddr[/length]</i>—View sessions with the specified destination IPv6 address. • source-port <i>num</i>—View sessions with the specified source port (1-65535). • source-v4-addr <i>ipaddr[/length]</i>—View sessions with the specified source IPv4 address. • source-v6-addr <i>ipaddr[/length]</i>—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.
filter { <i>name</i> config }	Displays information about configured session filters. Specify config to view all configured session filters, or specify a filter <i>name</i> 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 <i>num</i>—View sessions with the specified destination port (1-65535). • dest-v4-addr <i>ipaddr[/length]</i>—View sessions with the specified destination IPv4 address. • source-port <i>num</i>—View sessions with the

Parameter	Description
	specified source port (1-65535). • source-v4-addr <i>ipaddr[/length]</i>—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 <i>num</i>—View sessions with the specified destination port (1-65535). • dest-v6-addr <i>ipaddr[/length]</i>—View sessions with the specified destination IPv6 address. • source-port <i>num</i>—View sessions with the specified source port (1-65535). • source-v6-addr <i>ipaddr[/length]</i>—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 [<i>type</i> [<i>suboptions</i>	Displays session persistence information. The following persistence types can be specified: • dst-ip—Displays destination-IP persistent

Parameter	Description
]]	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 <code>aFlex persist uie</code> command. The available <i>suboptions</i> are the same as the ones for ipv4. NOTE: To clear persistent sessions, use the <code>clear sessions persist</code> command.
quic	Displays QUIC session information.
radius	Displays RADIUS session information.
sctp	Displays SCTP sessions only.
server [<i>name</i>]	Displays sessions for real servers, or a specific server <i>name</i> .
sip	Displays information for Session Initiation Protocol (SIP) sessions. The following suboptions are available: • dest-port <i>num</i>—View sessions with the specified destination port (1-65535). • dest-v4-addr <i>ipaddr[/length]</i>—View sessions with the specified destination IPv4 address. • dest-v6-addr <i>ipaddr[/length]</i>—View sessions with the specified destination IPv6 address. • smp-sip-rtp <i>num</i>—View SIP sessions.
sixrd-nat64	Displays 6rd-NAT64 session statistics. The available suboptions are the same as for ds-lite .
virtual-	Displays sessions for virtual servers, or a specific

Parameter	Description
server [<i>name</i>]	virtual server <i>name</i> .

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.

Field	Description
	This counter applies specifically to IP protocol load balancing. For more information, see “IP Protocol Load Balancing” chapter in the <i>Application Delivery and Server Load Balancing Guide</i> .)
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 Conn	Number of Layer 4 sessions currently available.
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	

Field	Description
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 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 (<code>incl-sport</code>) 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

Field	Description
	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. • 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 <i>is not</i> 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.

Field	Description
	• 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 12](#) describes the new fields in the command output.

Table 12 : 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 13](#) describes the new fields in the command output.

Table 13 : 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#.
```

NOTE: Data displayed for the “show shutdown” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650.
For Thunder 7650, the output is displayed only for one processing unit. For Thunder 14045 ACOS device, the output is displayed only for Master.

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: 80001f880439383736353433323130 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 <i>svr-name</i>	Returns OIDs for the axServerStatTable. If a <i>name</i> is specified, this command returns OIDs for the axServerPortStatTable.
service-group <i>sg-name</i>	Returns OIDs for the axServiceGroupStatTable. If a <i>name</i> is specified, this command returns OIDs for the axServerPortStatTable. You can narrow the command output by specifying

Parameter	Description
	the IP address type for addr-type or specific service-group <i>member</i> . Valid address types are firewall , tcp , or udp .
virtual-server <i>vs-name</i>	Returns OIDs for the axVirtualServerStatTable. If a <i>name</i> is specified, this command returns OIDs for the axVirtualServerPortStatTable.
port <i>port-num</i>	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 sgl: 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 sgl server-member s1
OID for axServiceGroupMemberStatTable
service-group-name sgl: 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 <i>profile-name</i>	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.

Parameter	Description
partition { shared <i>partition-</i> <i>name</i> }	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 AX 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
<code>debug</code>	View debug information.
<code>mac-table</code>	View the MAC addresses configured on the ASIC.
<code>vlan-table</code>	View the VLANs configured on the ASIC.
<code>xfp-temp</code>	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 “detail” option is used 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
```

- NOTE:** By default, data displayed for the “show system app-performance” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045 and TH7650. It will contain per-slot information for debug or tracking.
- For Thunder 7650, the output is displayed only for one Processing Unit. For Thunder 14045 ACOS device, the output is displayed only for Master.

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 [<i>file-name</i>]	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 <i>ipaddr</i>	Displays geo-location database entries for the specified IP address. • statistics – Displays client statistics for the specified geo-location. • policy <i>policy-name</i> – Filter output by policy.
ipv6 <i>ipv6addr</i>	Displays geo-location database entries for the specified IPv6 address. • statistics – Displays client statistics for the specified geo-location. • policy <i>policy-name</i> – Filter output by policy.
rdt [<i>options</i>]	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 <i>site-name</i> – Displays aRDT data only for the specified GSLB site. • depth <i>num</i> – 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
```

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”. <pre>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</pre>
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
-----
0          0    GR      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 RxD-Tx 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 RxD-Tx 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
<code>buffer-stats</code>	Shows counters for buffer statistics.
<code>cpu-packet-statistics</code>	Shows per-CPU packet statistics.
<code>busy-counter</code>	Shows counters for system busy statistics.
<code>interface-stats</code>	Shows counters for interface statistics.
<code>statistics</code>	Shows counters for internal statistics.
<code>te-mac</code>	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 Display the port list.

Syntax `show system port-list`

Mode All

show system radius server

Description Show configuration information or statistics for the ACOS RADIUS server.

Syntax `show system radius server {config | statistics}`

Parameter	Description
<code>config</code>	Displays the configuration for the ACOS RADIUS server.
<code>statistics</code>	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 <i>string</i>	Shows entries only for IMEI numbers.
imsi <i>string</i>	Shows entries only for IMSI numbers.
inside-ip <i>ipaddr</i>	Shows entries only for inside IP addresses.
msisdn <i>string</i>	Shows entries only for MSISDN numbers.
<i>custom-attr-name</i> [starts-with] <i>string</i> [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			
waf-template-count	650	128	32
1024			
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.

Field	Description
Maximum	Maximum number of resources that can be 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 configurable 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.

Field	Description
ipsec-sa-number	The number of IPsec SAs allowed.
waf-template-count	The total number of WAF templates available for configuration in the system.
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
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:             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.
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
```

NOTE:

Data displayed for the “show system-ssl status” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650. This will not contain the dynamic data, per-slot information like. For per-slot information, select “detail” option:

- **Number of CPUs:** If one processing unit has 48 cores, then it will show as 96.
- **Total Storage Space:** If one processing unit has 100G, then the total will be shown as 200G.
- **Total Memory Space:** If one processing unit has 250GB, then the total will be shown as 500G.

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
<i>hostname</i>	Only display information for the server with the specified host name.
<i>ipaddr</i>	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
<code>export</code>	Exports the output to a remote server.
<code>use-mgmt-port</code>	Uses the management port to perform the export.
<code>url</code>	Specify 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. To enter the entire URL: • <code>tftp://host/file</code> • <code>ftp://[user@]host[:port]/file</code> • <code>scp://[user@]host/file</code> • <code>sftp://[user@]host/file</code>

Option	Description
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

Field	Description
	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 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.

Field	Description
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
```

NOTE: Data displayed for the “show version” CLI output has been consolidated to provide a single output for chassis platforms i.e. TH14045, TH7650. It will contain doubled static values as total memory, CPUs, and storage. But it will not contain dynamic data information as free storage and memory. For Thunder 7650, the output is displayed only for one processing unit. For Thunder 14045 ACOS device, the output is displayed only for Master.

show vlans

Description Display the configured VLANs.

Syntax `show vlans [vlan-id]`

Parameter	Description
<i>vlan-id</i>	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
SVLAN Partition switched	The number of SVLAN partition

Parameter	Description
counter	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
<i>vlan-id</i>	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 VPN 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 Clear DNS caching information.

Syntax

```
clear dns cache
[client |
entry [dns-class string | dns-type string | domain-name [dns-
domain-name | fqdn-domain] name] |
global [dns-class string | dns-type string | domain-name [dns-
domain-name | fqdn-domain] name] |
statistics]
```

Parameter	Description
client	Clear DNS client statistics.
entry	Clear DNS cache entries for one of the filters given below: dns-class - You can specify one of the following

Parameter	Description
	DNS classes: ◦ IN – INTERNET class ◦ CH – CHAOS class ◦ HS – HESIOD class ◦ NONE – NONE class ◦ ANY – ANY class ◦ <i>num</i> - 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 ◦ <i>num</i> - Other type value (1-65535) • domain - You can specify either one of the following: ◦ dns-domain-name – Domain name ◦ fqdn-domain – Fully qualified domain name
global	Clear DNS cache global entries for one of the filters given below:

Parameter	Description
	• 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 ◦ <i>num</i> - 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 ◦ <i>num</i> - Other type value (1-65535) • domain - You can specify either one of the following: ◦ dns-domain-name – Domain name ◦ fqdn-domain – Fully qualified domain name
statistics	Clear DNS caching statistics.

Mode Privileged EXEC mode or global configuration mode

Example The following command clears DNS caching statistics:

```
ACOS# clear dns cache statistics
```

Example The following command clears the global DNS cache based on the domain name:

```
ACOS# clear dns cache global domain-name dns-domain-name  
foo.com
```

Example The following command clears the system DNS cache for DNS type CNAME:

```
ACOS# clear dns cache entry dns-type CNAME
```

Example The following command clears the system DNS cache for DNS class 55:

```
ACOS# clear dns cache entry dns-class 55
```

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 serviceipl  
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
<code>arp ipv4-fib ipv6-fib mac nd6</code>	Sync ARP/MAC/ND6 tables across all the partitions. IPv4/IPv6 FIB will only be synced for the shared partition.
<code>ipv4-fib ipv6-fib</code>	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
<i>partition-name</i>	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
<i>partition-name</i>	Specifies the name of the L3V partition.
id <i>num</i>	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
<code>access { axapi cli web }</code>	Configure the access type, i.e., specify the user interfaces through which the partition admin can access the partition. The following options are available: • <code>axapi</code> - Allow access through aXAPI. • <code>cli</code> - Allow access through command line interface. • <code>web</code> - Allow access through Web GUI. By default, access is allowed through all user interfaces (CLI, GUI, and aXAPI).
<code>disable</code>	Disables the partition admin user account. By default, the partition admin user accounts are enabled when they are added.
<code>enable</code>	Enables the partition admin user account. By default, the partition admin user accounts are enabled when they are added.
<code>password string</code>	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 .)
<code>privilege level</code>	Configures the privileges for the user account. The following options are available: <code>partition-read</code> – The user has read-only privileges within the L3V partition. <code>partition-write</code> – The user has read-write privileges within the L3V partition. <code>partition-enable-disable</code> – 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 <i>For more information, see Configuring Application Delivery Partitions guide.</i> The default privilege is <code>partition-read</code>.
<code>trusted-host { ipaddr/mask- length ipaddr subnet-mask }</code>	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-group group-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	Adds a partition to the group.
<i>partition-name</i>	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
<i>partition-name</i>	Specifies the name of the service partition.
id <i>num</i>	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 <i>adc</i>	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
<code>vlan</code> <i>vlan_id</i>	VLAN ID to use for the Shared VLAN feature. This VLAN must be configured as a shared VLAN ahead of time.
<code>allowable-ip-range</code> <i>ip</i>	IPv4 addresses in this range are used for configuring VE interfaces in partitions and for <code>mgmt-floating-ip address</code> configurations. The command <code>allowable-ip-range 1.3.4.0/24</code> 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 <code>shared-vlan</code> feature. Any VIP address configured in partition P1 inside the range of 1.3.4.0/24 cannot be configured with <code>vr-id</code> in its partition, because partitions using shared partition feature always use the <code>vr-id</code> follow feature in the partition.
<code>allowable-ipv6-range</code> <i>ip</i>	The command <code>allowable-ipv6-range 1111::0/64</code> 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 <code>shared-vlan</code> feature. Any VIP address configured in partition P1 inside the range of 1111::0/64 cannot be configured with <code>vr-id</code> in its partition, because partitions using shared partition feature always use the <code>vr-id</code> follow feature in the partition.
<code>mgmt-floating-ip-address</code> <code>ip vrid</code> <code>vrid_id</code>	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 <code>mgmt-floating-ip-address</code>. The vMaster owns this IP address and is used to configure all the devices. The <code>vrid</code> given with this configuration must also be used in <code>affinity-vrrp-a-vrid vrid</code>. It is preferred to use the configuration system <code>ve-mac-scheme system-mac</code>, while configuring the shared VLAN feature. The configuration <code>system ve-mac-scheme system-mac</code> uses the Mac based lookup to identify the L3V Partition id and this lookup is much faster. The configuration <code>system ve-mac-scheme system-mac</code> 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
<code>all</code>	View all partitions on the device, both active and inactive. Without this option, only active partitions are displayed.
<code>available-id</code>	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.
<code>port-ownership</code>	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. <code>aflex-scripts</code> - This parameter is also available for viewing aFlex scripts along with the partitions.
shared	View the running-config for the shared partition only.
<i>name</i>	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 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 Virtual Chassis System (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 <code>router device-context</code> command in previous releases.
Syntax	<pre>device-context <i>DeviceID</i></pre>

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 virtual chassis.

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
<code>enable</code>	Enables database cluster distribution.
<code>disable</code>	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
```

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 Enable 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 chassis, 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
<code>[no] affinity-vrrp-a-vrid</code>	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
<i>vrid-group</i>	cluster, including the Active device.
[no] enable	Enables aVCS on the device. aVCS is disabled by default.
[no] interfaces { ethernet <i>portnum</i> management trunk <i>trunk-num</i> ve <i>ve-num</i> }	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 chassis must be able to reach the device on the specified interface(s).
[no] priority <i>num</i>	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 <i>portnum</i>	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 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 chassis. 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
<i>Unicast</i>	Enables aVCS Unicast election mode.
<i>Mcast</i>	Enables aVCS Multicast election mode.
<i>Mixed</i>	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	Enable aVCS on the device.
Syntax	<code>vcs enable</code>
Default	N/A. This is an operational command rather than a configuration command.
Mode	Privileged EXEC (vMaster or vBlade)
Usage	After you enter the <code>vcs enable</code> command, you must enter the <code>vcs reload</code> 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
<i>retries</i>	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 chassis 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 virtual chassis.

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 virtual chassis 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 virtual chassis.

Syntax	<code>[no] vcs floating-ipv6 ipv6-addr/mask-length</code>
	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 virtual chassis to the IPv6 address <code>fc00:0:3::23:a/24</code> :

```
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	<code>[no] vcs force-wait-interval seconds</code>
	Replace <i>seconds</i> 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	<code>[no] vcs hold-preemption-interval <num></code>

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 Multi-PU platforms.
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	<pre>[no] vcs multicast-ip ipv4-addr</pre> Replace <i>ipv4-addr</i> 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	<pre>[no] vcs multicast-ip ipv6-addr</pre> Replace <i>ipv6-addr</i> 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	<pre>[no] vcs multicast-port portnum</pre> Replace <i>portnum</i> 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	<pre>[no] vcs offload upgrade protocol <scp></pre>
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 chassis.
db-safe	During the vcs reload process, the db-safe option ensures that Scaleout is stable and the traffic is uninterrupted. • <i>start</i> - VCS enters the db-safe reload mode. In this mode, Scaleout remains stable and ignores any node leaving or joining. ◦ <i>timeout</i> - 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 <code>vcs reload db-safe start</code> option is used without the timeout option, then the db-safe mode ends automatically after the vcs reload process completes. • <code>complete</code> - This option completes the db-safe reload mode. It must be used on PU1. ◦ <code>force</code> - 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 <code>force</code> option to complete the db-safe mode forcefully.
<code>device</code>	The <code>device</code> option reloads a specific device when aVCS is enabled. The device ID can be between 1-16.
<code>disable-merge</code>	The <code>disable-merge</code> option prevents configuration information from being migrated from PU2 to PU1 following the reload. Use this option when you are replacing a virtual chassis 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 chassis 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 chassis:

```
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
<code>ip-address</code>	Adds the IPv4 address of the member for aVCS unicast election.
<code>ipv6-address</code>	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
<code>port</code>	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	<pre>vcs vMaster-maintenance <i>period</i></pre> Replace <i>period</i> 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 virtual chassis 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 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.
Floating IP	Floating IP of the virtual chassis.
Mask	Mask address of the virtual chassis.
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 <code>show vcs summary</code> 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
<i>cpu_number</i>	Specify the target number of CPUs on the destination. The number ranges from 1 through 75.
<i>target_ip_address</i>	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
<code>migration</code>	
<code>finish migration</code>	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 Change 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.

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	<code>[no] device-id num</code> Replace <i>num</i> 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 <code>no enable</code> command in release 4.0.
Syntax	<code>disable</code>
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	<code>[no] disable-default-vrid</code>
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	Configure 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
Mode	VRRP-A common configuration mode

Usage This command applies only to the shared partition.

Example Set the delay interval to 20 seconds (200 100-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
```

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-port port | preferred-trunk trunk}`

Parameter	Description
<i>port</i>	Ethernet port number.
<i>trunk</i>	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 Change the delay waited by the ACOS Device before beginning failover in response to priority changes.

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 2 seconds (20 100-millisecond units).

```
ACOS(config)# vrrp-a common
ACOS(config-common)# track-event-delay 20
```

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
<pre>[no] gateway gateway-IP- address weight value</pre>	Specify the IP Address of an IPv4 or IPv6 default gateway that has also been configured as a real server, such as <code>ACOS(config)#slb server GW1</code> or <code>ACOS(config)#cgnv6 server GW1</code>. 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.
<pre>[no] interface interface- type interface- number weight value</pre>	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.
<pre>[no] route route- number subnet weight value [distance num] [gateway ip] [protocol {any static dynamic}]</pre>	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 <i>trunk-id</i> weight <i>value</i> per-port-weight <i>value</i>	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 <i>vlan-id</i> timeout <i>timeout-value</i> weight <i>value</i>	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 <i>num</i>	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	<code>[no] vrrp-a force-self-standby-persistent [vrid num]</code> Replace <i>num</i> 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
<i>port-num</i>	Configures the specified interface as the VRRP-A interface.
<i>trunk-num</i>	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 <i>vlan-id</i>	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
<i>port-num</i>	Configure the specified ethernet port to receive sync sessions.

Parameter	Description
<i>trunk-num</i>	Configure the specified trunk port to receive sync sessions.
<i>vlan-id</i>	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 { <i>port</i> <i>range_of_ports</i> }	Configure one or many VRRP-A interface ports to restart.
vrid <i>num</i>	Enters a VRID sub-configuration mode where the ethernet port or range is also available: 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	<pre>[no] vrrp-a vrid num</pre> 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	<pre>[no] vrrp-a session-sync</pre> 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	<pre>[no] vrrp-a vrid num</pre> 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
<i>ipaddr</i>	The IPv4 address of the floating IP.
<i>ipv6addr</i>	The IPv6 address of the floating IP. • <i>ethernet id</i> - Ethernet interface. Visible in the shared partition. • <i>trunk id</i> - Trunk interface. Visible in the shared partition. • <i>ve id</i> - 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	Disable preempt mode.
threshold <i>num</i>	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 60 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

NOTE: This command is changed from release 4.0, where it was available under VRRP-A VRID 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	<pre>[no] gateway {ipaddr ipv6addr} priority- costnum</pre>	Configure tracking for the IPv4 or IPv6 default gateways. If a gateway fails, the specific <i>num</i> will be subtracted from the priority on the VRID.
Interface	<pre>[no] interface ethernet num priority- costnum</pre>	Configure tracking for a specified interface. If the interface fails, the specific <i>num</i> will be subtracted from the priority on the VRID.
Route	<pre>[no] route {ipaddr ipv6addr} {/mask- length subnet- mask} [priority- costnum] [distance num] [gatewayip] [protocol {any static dynamic}]</pre>	Configure tracking for the specified route. If the specified route is missing, the specific <i>num</i> 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	<code>[no]</code> <code>trunk</code> <code>num</code> <code>priority-</code> <code>costnum</code> <code>[per-port-</code> <code>pri num]</code>	Configure tracking for a specified trunk. If the trunk or individual ports on the trunk fail, the specified priority cost <i>num</i> will be subtracted from the priority on the VRID. The <code>per-port-pri</code> option tracks individual ports in the trunk. The VRID's priority is reduced by the <code>per-port-pri</code> amount for each port that fails.
VLAN	<code>[no]</code> <code>vlanvlan-</code> <code>id</code> <code>timeout</code> <code>seconds</code> <code>priority-</code> <code>costnum</code>	Configure tracking for the specified VLAN. If traffic is no longer detected on the specified VLAN, the specific <i>num</i> will be subtracted from the priority on the VRID. The <code>timeout</code> 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	<code>show vrrp-a [detail]</code>
Mode	All
Usage	This command is only valid in the shared partition.
Example	The following example shows sample output for the <code>show vrrp-a</code> 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 templatel
    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 chassis platform.

Syntax `show vrrp-a te-mac`

Mode All

Usage This command is supported only on the chassis 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
<i>partition-name</i>	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 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
<code>enable</code>	Enables the distributed forwarding for the firewall.
<code>disable</code>	Disables the distributed forwarding for the firewall. This is the default option.
<code>session-offload-direction</code>	Configures the session offload direction. • <code>uplink</code> – Enables the session offload only in the uplink direction. • <code>downlink</code> – Enables the session offload in the downlink direction. • <code>Both</code> – Enables the session offload in both directions. This is the default option.
<code>threshold</code>	Configures the packet threshold value to offload the session. The value can be 4 – 63. The default value is 5. • <code>udp</code> – Configures the threshold for the udp session offload. • <code>tcp</code> – 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
```


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
<code>route-aggregation</code>	By default, the NAT IPs are aggregated and then allocated to a user group. The aggregated NAT IPs are advertised as a single route.
<code>mod-user-groups</code>	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
```

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.

Parameter	Description
	• <code>ipv6</code> - 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 to determine the reachability options

Parameter	Description
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

Parameter	Description
	state based on the relevant tracking templates: • <code>ipv4</code> – matched when the state of the IPv4 tracking template goes up/down or the default tracking template goes up/down. • <code>ipv6</code> – 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.

Parameter	Description
	• <i>inside-user</i> - Displays inside user to user group mapping information. • <i>nat-address</i> - Displays NAT IP to user group mapping information. • <i>nat-pool</i> - Displays user group mapping information for all NAT IPs in a NAT pool. • <i>fixed-nat</i> - 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 <code>show cgnv6 fixed-nat detail</code> 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 <code>show scaleout</code> 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)

Field	Description
	• 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 <code>show scaleout</code> 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 Mismatch 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
Received 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 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.
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 standby for the corresponding 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	The number of packets received by the cluster

Field	Description
active drop	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 standby 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 error dest mac zero drop	The packets dropped since the destination mac 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 encaps 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.

Field	Description
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 Error	The packets dropped since error occurred while trying to fragment the packet.
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	The packets dropped since it is a IPv6 jumbo packet and needs fragmentation.

Field	Description
drop	
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

Old Output	New Output
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
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

Old Output	New Output
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 Destination Mac Error	L3 Redirect RX multi-slot Destination 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

Old Counter Names	New Counter Names
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
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
```



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
<i>list-name</i>	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
<code>[no] priv-addr/mask-length {glid num lid num lsn-lid num lsn-radius-profile num}</code>	Specifies the internal clients. The <code>priv-addr</code> option specifies the internal host or subnet address. The <code>/mask-length</code> specifies the network mask or mask length. • The glid<i>num</i> option specifies an global LSN LID to apply to matching clients. • The lid<i>num</i> option specifies a non-LSN LID to apply to matching clients. • The lsn-lid<i>num</i> option specifies an LSN LID to apply to matching clients. • The lsn-radius-profile <i>num</i> 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
```

cgenv6 enable-port-batch-v1

Description Enable Port Batching v1.

Syntax	<code>[no] cgnv6 enable-port-batch-v1</code>
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	<code>[no] cgnv6 ecmp 4-tuple-hash</code>
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	<code>[no] cgnv6 global domain-list [interval <i>minutes</i> fail-interval <i>seconds</i> aaaa-query { enable disable }]</code>

Parameter	Description
<code>interval <minutes></code>	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 <i><seconds></i>	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 <code>cgnv6 logging pool-based log cycle 0</code> 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	

cgenv6 lsn alg

Description Disables or re-enables Application Level Gateway (ALG) support for LSN and Fixed-NAT.

Syntax

```
[no] cgenv6 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

cgenv6 lsn alg sip rtp-stun-timeout

Description Change the RTP/RTCP Session Traversal Utilities for NAT (STUN) timeout for full-cone sessions.

Syntax `[no] cgenv6 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
<code>tcp udp</code>	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: <code>port</code> configures a single destination port or Port Range Start <code>session-limit</code> 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.

cgenv6 lsn endpoint-independent-mapping

Description Configure endpoint-independent mapping for both ephemeral and well-known ports.

Syntax `[no] cgenv6 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.

cgenv6 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
<code>filter-none</code>	Allows for self-hairpinning for UDP packets only. This is the default behavior for UDP packets.
<code>filter-self-ip</code>	Drops packets that have the same inside client IP address for both the source and destination.
<code>filter-self-ip-port</code>	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

cgenv6 lsn half-close-timeout

Description Configure the TCP half-closed session timeout for LSN.

Syntax `[no] cgenv6 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](#).

cgenv6 lsn health-check-gateway

Description Configure enforcement of gateway health monitoring prior to redistributing LSN NAT pool prefixes.

Syntax `[no] cgenv6 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.

cgenv6 lsn icmp

Description Send ICMP Destination Unreachable messages when there are no protocol ports available for NAT mappings, or when a user quota is exceeded.

Syntax `[no] cgenv6 lsn icmp
{send-on-port-unavailable |`

```

send-on-user-quota-exceeded}
{
admin-filtered |
disable |
host-unreachable
}

```

Parameter	Description
<code>send-on-port-unavailable</code>	Sends ICMP Destination Unreachable message when there are no protocol ports available for NAT mappings.
<code>send-on-user-quota-exceeded</code>	Sends ICMP Destination Unreachable message when a a user quota is exceeded.
<code>admin-filtered</code>	Sends code type 3, code 13, administratively filtered.
<code>disable</code>	Disable ICMP Unreachable messages for the specified event.
<code>host-unreachable</code>	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

cgenv6 lsn inbound-refresh

Description Enable or disable the session aging time for NAT translation.

Syntax `[no] cgenv6 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.

cgenv6 lsn inbound-refresh-full-cone

Description Enable or disable the session aging time for LSN full-cone sessions.

Syntax	<code>cgenv6 lsn inbound-refresh-full-cone {disable enable}</code>
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.

cgenv6 lsn inside source class-list

Description	Bind an IP class list for use with LSN.
Syntax	<code>[no] cgenv6 lsn inside source class-list <i>list-name</i></code> Replace <i>list-name</i> 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.

cgenv6 lsn ip-selection

Description	Specify the method for LSN to use to select IP addresses within a pool.
Syntax	<code>[no] cgenv6 lsn ip-selection <i>method</i></code> Replace <i>method</i> 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.

cgenv6 lsn logging default-template

Description	Set a configured LSN traffic logging template as the default template for all LSN pools.
Syntax	<pre>[no] cgenv6 lsn logging default-template <i>template-name</i></pre> Replace <i>template-name</i> 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.
<i>Name</i>	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
<i>pool-name</i>	Specifies the LSN pool.
<i>template-name</i>	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
<code>tcp udp</code>	Enable or disable port overloading behavior for TCP or UDP traffic specifically.
<code>port-num [to port-num]</code>	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
<i>priv-ipaddr</i>	Specifies the internal IP address.
<i>start-priv-portnum</i>	Specifies the beginning (lowest-numbered) protocol port number in the range of internal protocol port numbers.
<i>end-priv-portnum</i>	Specifies the ending (highest-numbered) protocol port number in the range of internal protocol port numbers.
<i>public-ipaddr</i>	Specifies the public IP address to map to the internal IP address.
<i>start-public-</i>	Specifies the beginning public protocol port number in the range to map to the internal protocol port

Parameter	Description
<i>portnum</i>	numbers.
<i>end-public-portnum</i>	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

cgenv6 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] cgenv6 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.

cgenv6 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] cgenv6 lsn stun-timeout {tcp | udp} port port-num [to port-num] minutes`

Parameter	Description
<code>tcp udp</code>	Specifies the Layer 4 protocol. If you omit this option, the command applies to both TCP and

Parameter	Description
	UDP.
port <i>port-num</i> [to <i>port-num</i>]	Specifies an individual port or a custom port range.
<i>minutes</i>	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.

cgnav6 lsn syn-timeout

- Description** Configure the SYN timeout for LSN.
- Default** `[no] cgnav6 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.

cgnav6 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] cgnav6 lsn tcp mss-clamp {none | fixed n | subtract s [min n] }`

Parameter	Description
none	Does not change the MSS value.
fixed <i>n</i>	Changes the MSS to the length you specify.
subtract <i>s</i>	Reduces the MSS if it is longer than the specified

Parameter	Description
<code>[min n]</code>	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

cgnav6 lsn tcp reset-on-error

Description Send TCP resets to LSN clients in response to invalid TCP packets from the inside network.

Syntax `[no] cgnav6 lsn tcp reset-on-error outbound disable`

Default Enabled

Mode Configuration mode

cgnav6 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-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.

Command	Description
<code>[no] conn-rate-limit <i>num</i></code>	The maximum number of connections a client can attempt to initiate per second. The value can range from 1-65535.
<code>[no] ds-lite inside-src-permit-list <i>list-name</i></code>	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.
<code>[no] extended-user-quota {tcp udp} service-port <i>portnum</i> sessions <i>num</i></code>	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.
<code>[no] lsn-rule-list destination <i>list-name</i></code>	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
<code>[no] name</code> <i>string</i>	Assigns a name to the LID.
<code>[no]</code> <code>override</code> { <code>none</code> <code>drop</code> <code>pass-through</code> }	Overrides NAT for matching traffic, and performs the specified action instead: • <code>none</code> – Applies source NAT if configured (default). • <code>drop</code> – Drops the traffic. • <code>pass-through</code> – Forwards the traffic without performing NAT.
<code>[no]</code> <code>respond-to-</code> <code>user-mac</code>	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.
<code>[no] source-</code> <code>nat-pool</code> <i>pool-name</i>	Binds an LSN NAT pool to the LID.
<code>[no] user-</code> <code>quota</code> { <code>tcp</code> <code>udp</code> <code>icmp</code> <code>session</code> <code>session-tcp</code> <code>session-udp</code> } <i>quota-num</i> <code>[reserve</code> <i>reserve-num]</i>	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 <code>reserve</code> 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 <code>reserve</code> can be configured only for user-quota tcp and user-quota udp.

Command	Description
	Configures user quota based on sessions: • <code>session</code> - Configures user quota for the number of data sessions. It can be 1-2147483647. • <code>session-tcp</code> - Configures user quota for the number of TCP sessions. It can be 1-2147483647. • <code>session-udp</code> - Configures user quota for the number of UDP sessions. It can be 1-2147483647.
<code>[no] user-quota-prefix-length</code> <i>length-num</i>	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 <i>attribute-type</i> } [exact-value <i>string</i> starts-with <i>string</i>] lsn-lid <i>num</i>	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 <i>attribute-type</i> can be one of the following: • default – Matches on clients who do not have any of the following custom attributes. • msisdn – Matches on client MSISDN. • 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 <i>string</i> – Matches only on an exact attribute value. • starts-with <i>string</i> – 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
<code>[no] default</code>	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. • <code>[no]dscp[any dscp-value]action set-dscp {inbounddscp-value [outbounddscp-value] outbounddscp-value [inbounddscp-value]}</code> • <code>[no] icmp {action action no-action}</code>

Command	Description
	◦ dnat ipv4-list <i>list-name</i> {action <i>action</i> no-action} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] others {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> {no <i>action</i> no-action} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] tcp port {0 <i>portnum</i> [to <i>portnum</i>]} ◦ [no] tcp port {0 <i>portnum</i> [to <i>portnum</i>]} ◦ dnat ipv4-list <i>list-name</i> {no-snat port-list <i>num</i>} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]}

Command	Description
	◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} ◦ template http-alg <i>template-name</i>
[no] default	• [no] udp port {0 <i>portnum</i> [to <i>portnum</i>]} {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> {no-snat port-list <i>num</i>} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>}
[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 <i>string</i>	Enters the configuration level for the set of rules to apply to the specified domain list name. • [no]dscp[any <i>dscp-value</i>]action set-dscp {inbound<i>dscp-value</i> [outbound<i>dscp-value</i>] outbound<i>dscp-value</i> [inbound<i>dscp-value</i>]} • [no] icmp {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through

Command	Description
	◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] others {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] tcp port {0 <i>portnum</i> [to <i>portnum</i>]} {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> {no-snat port-list <i>num</i>} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} ◦ template http-alg <i>template-name</i>
[no] domain- list-name <i>string</i>	• [no] udp port {0 <i>portnum</i> [to <i>portnum</i>]} {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> {no-snat port-list <i>num</i>}

Command	Description
	◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>}
[no] domain-name <i>string</i>	Enters the configuration level for the set of rules to apply to the specified domain name. • [no]dscp{any <i>dscp-value</i>}action set-dscp {inbound<i>dscp-value</i> [outbound<i>dscp-value</i>] outbound<i>dscp-value</i> [inbound<i>dscp-value</i>]} • [no] icmp {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] others {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]}

Command	Description
	◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] tcp port {<i>0</i> <i>portnum</i> [<i>to portnum</i>]} {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> {no-snat port-list <i>num</i>} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} ◦ template http-alg <i>template-name</i>
[no] domain-name <i>string</i>	• [no] udp port {<i>0</i> <i>portnum</i> [<i>to portnum</i>]} {action <i>action</i> no-action} ◦ dnat ipv4-list <i>list-name</i> {no-snat port-list <i>num</i>} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> [outbound <i>dscp-value</i>] outbound <i>dscp-value</i> [inbound <i>dscp-value</i>]} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>}
[no] http-match- domain-name	Enables matching domain name in the HTTP request.
[no] ip <i>ipv4addr</i> <i>/mask-</i>	Enters the configuration level for the set of rules to apply to the specified IP host address or subnet.

Command	Description
<i>length</i>	• [no] dscp {{any <i>dscp-value</i>} action set-dscp {inbound <i>dscp-value</i> outbound <i>dscp-value</i>}} • [no] default {action <i>action</i> no-action} Replace <i>action</i> with the following options: ◦ dnat {domain <i>domain-name</i> ipv4-list <i>list-name</i>} ◦ drop ◦ one-to-one-snat {pool <i>pool-name</i>} ◦ pass-through ◦ set-dscp { inbound <i>dscp-value</i> outbound <i>dscp-value</i>} ◦ snat {pool [<i>pool-name</i> <i>pool-group-name</i>]} • [no] icmp {action <i>action</i> no-action} Replace <i>action</i> with the following options: ◦ dnat {domain <i>domain-name</i> ipv4-list <i>list-name</i>} ◦ drop ◦ one-to-one-snat {pool <i>pool-name</i>} ◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> outbound <i>dscp-value</i> } ◦ snat {pool [<i>pool-name</i> <i>pool-group-name</i>]} • [no] others {action <i>action</i> no-action} Replace <i>action</i> with the following options: ◦ dnat {domain <i>domain-name</i> ipv4-list <i>list-name</i>} ◦ drop

Command	Description
	◦ one-to-one-snat <i>pool pool-name</i> ◦ pass-through ◦ set-dscp {<i>inbound dscp-value</i> <i>outbound dscp-value</i>} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} • [no] tcp { port {0 <i>portnum</i> { [to <i>portnum</i>] action <i>action</i> no-action } } } Replace <i>action</i> with the following options: ◦ dnat {<i>domain domain-name</i> ipv4-list <i>list-name</i> {no-snat {<i>vrid vrid</i>} port-list <i>port-list-name</i> {no-snat {<i>vrid vrid</i>}}} ◦ drop ◦ one-to-one-snat pool <i>pool-name</i> ◦ pass-through ◦ set-dscp {<i>inbound dscp-value</i> <i>outbound dscp-value</i>} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>} ◦ idle-timeout {<i>num</i> <i>fast</i>} ◦ template http-alg <i>template-name</i>
[no] ip <i>ipv4addr</i> <i>/mask-length</i>	• [no] udp{port{0 <i>portnum</i> { [to <i>portnum</i>] action <i>action</i> no-action } } } Replace <i>action</i> with the following options: ◦ dnat {<i>domain domain-name</i> ipv4-list <i>list-name</i> {no-snat {<i>vridvrid</i>} port-list <i>port-list-name</i> {no-snat {<i>vrid vrid</i>}}} ◦ drop ◦ one-to-one-snat {<i>pool pool-name</i>}

Command	Description
	◦ pass-through ◦ set-dscp {inbound <i>dscp-value</i> outbound <i>dscp-value</i> } ◦ idle-timeout {<i>num</i> fast} ◦ snat pool {<i>pool-name</i> <i>pool-group-name</i>}

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
al0rocks.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	<code>[no] cgnv6 nat icmp always-source-nat-errors</code>
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	<code>[no] cgnv6 nat icmp respond-to-ping</code>
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	<code>[no] cgnv6 nat icmpv6 respond-to-ping</code>

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
<i>pool-name</i>	Name of the address pool.
<i>start-ipaddr</i>	Beginning (lowest) IP address in the range.
<i>end-ipaddr</i>	Ending (highest) IP address in the range.
netmask { <i>subnet-mask</i> <i>/mask-length</i> }	The netmask <i>/mask-length</i> 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 <i>num</i>	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
<pre> 256 512 1024 2048 4096 }</pre>	• 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 <i>vrid</i>	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 <i>start-ipaddr</i> [to <i>end-ipaddr</i>]	Excludes the specified IP address or address range from the pool.

Default None.

Mode Configuration mode

cgenv6 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] cgenv6 nat pool-group pool-group-name`
`[vrid vrid]`

Parameter	Description
<i>pool-group-name</i>	Name of the pool group.
vrid <i>vrid</i>	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 <i>pool-name</i>	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, if 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
<code>tcp</code>	Configures the tcp port from which the specified ports are excluded from the NAT pool.
<code>udp</code>	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
<code>port</code>	Configures a single port or a starting port range to be excluded from the NAT pool.
<code>to Port Range</code>	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
```

cgenv6 one-to-one mapping-timeout

Description Configure a timeout value for the NAT one-to-one mapping.

Syntax `[no] cgenv6 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

cgenv6 one-to-one pool

Description Configure a named set of IP addresses for use by one-to-one NAT.

Syntax `[no] cgenv6 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] cgenv6 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
<i>pool-name</i>	Name of the address pool.
<i>start-</i>	Beginning (lowest) IP address in the range.

Parameter	Description
<i>ipaddr</i>	
<i>end-ipaddr</i>	Ending (highest) IP address in the range.
netmask { <i>subnet-mask</i> <i>/mask-length</i> }	The netmask <i>/mask-length</i> 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 <i>vrid</i>	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-group** *pool-group-name*
 [**vrid** *vrid*]

Parameter	Description
<i>pool-group-name</i>	Name of the pool group.
vrid <i>vrid</i>	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 <i>pool-name</i>	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	<pre>[no] cgnv6 port-list name [original-port num to translated-port num]</pre>

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)# cgnav6 port-list abc  
ACOS(config-port-list)# original-port 80 to translated-port 8080
```

cgnav6 resource-usage

Description Configure CGNAV6 resource usage.

Syntax

```
[no] cgnav6 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 CGNAV6 Fixed NAT inside users.
fixed-nat-ip-addr-count	Total configurable CGNAV6 Fixed NAT addresses
lsn-nat-addr-count	Total configurable CGNAV6 NAT Pool addresses
radius-table-size	Total configurable CGNAV6 RADIUS Table entries
stateless-entries	Helper size for CGN Stateless Technologies.

Default None.

Mode Configuration mode

cgenv6 sctp rate-limit

Description Configure a traffic rate-limit for SCTP sessions.

Syntax `[no] cgenv6 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.
<i>ip-addr</i>	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 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.

cgenv6 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] cgenv6 template http-alg template-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
<code>[no]</code> <code>request-</code> <code>insert-</code> <code>client-ip</code> <code>[options]</code>	Enables insertion of the client IP address into the headers of client HTTP requests. You can specify the following options: • header-name <i>string</i> – 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 <i>string</i> include-tunnel-ip header-name <i>string</i>] – 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.
<code>[no] request- insert- msisdn [options]</code>	Inserts the client’s mobile number in client requests. • header-name<i>string</i> – Header name to insert, instead of the default. The following option is available: ◦ radius-sg<i>group-name secretstring shared-secret</i> – Specifies the group of RADIUS accounting servers to use for obtaining client mobile numbers. • radius-sg<i>group-name secretstring shared-secret</i> – Specifies the group of RADIUS accounting servers to use for obtaining client mobile numbers. The following parameters are available: ◦ <i>group-name</i> – Name of the service group that contains the client RADIUS servers. ◦ <i>string</i> – Authentication string the ACOS device and the client RADIUS servers use to authenticate RADIUS traffic from one another. ◦ retry<i>num</i> – 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<i>num</i> – 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<i>seconds</i> – 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 <i>num</i> { <i>num</i> 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 <i>num</i>	Configure an idle-timeout for TCP traffic. You can specify a value in the range of 2-15000 seconds.
udp-timeout <i>num</i>	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
<code>[no] start-ipv4-addr to end-ipv4-addr</code>	Range of IPv4 addresses. Enter the lowest address number in the range first.
<code>[no] start-ipv6-addr to end-ipv6-addr</code>	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
<code>[no] destination {service-group <i>sg-name</i> <i>ip-addr</i>}</code>	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.
<code>disable</code>	Disable this NetFlow monitor.
<code>disable-log-by-destination</code>	Disable logging by destination protocol and port. The following options are available: <code>icmp</code> – Disable logging for icmp traffic. <code>others</code> – Disable logging for other L4 protocols. <code>tcp</code> – Disable logging by destination TCP port. <code>udp</code> – Disable logging by destination UDP port.
<code>[no] flow-timeout <i>minutes</i></code>	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.
<code>[no] protocol {v9 v10}</code>	Configure which version of the NetFlow protocol to use, version 9 or version 10. The default is NetFlow version 9.
<code>[no] record</code> <code>netflow-</code> <code>template-type</code> <code>[both </code> <code>creation </code> <code>deletion]</code>	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 <i>num</i> timeout <i>seconds</i> }	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 <i>string</i> ipv6 <i>string</i> }	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-filter filter-name set
{
  dest-addr portnum |
  dest-port portnum |
  ipv6 |
  sip |
  source-addr portnum |
  source-port portnum
}
```

Parameter	Description
<code>dest-addr</code> <i>portnum</i>	Matches on destination address.
<code>dest-port</code> <i>portnum</i>	Matches on destination port.
<code>ipv6</code>	Matches specifically on IPv6 addresses.
<code>sip</code>	Matches on SIP sessions.
<code>source-addr</code> <i>portnum</i>	Matches on source address.
<code>source-port</code> <i>portnum</i>	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]
[vrid vrid]
```

Parameter	Description
<i>ipv6-addr/nn</i>	Specifies the prefix.
class-list <i>list-name</i>	Specifies a class list of inside source parameters for the prefix.
vrid <i>vrid</i>	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
<code>[no] health-check {monitor-name}</code>	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.
<code>[no] health-check-disable</code>	Disables health monitoring of the server.
<code>[no] port port-num {tcp udp}</code>	Specifies the TCP or UDP port on which the server listens for traffic. enable disable Enables or disables the port. <code>[no] health-check [monitor-name]</code> Enables health monitoring of the port. The monitor-name option specifies the name of a configured

Command	Description
	health monitor. If you omit the <code>health-check</code> command or you enter it without the monitor-name option, the default UDP health monitor is used. <code>[no] health-check-disable</code> 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
<code>[no] health-check</code> <code>[monitor-name]</code>	Enables health monitoring of the service group. The monitor-name specifies the name of a configured health monitor.
<code>[no] member</code> <code>{member-name}</code> <code>{portnum}</code>	Adds the external log server and port to the service group.
<code>[no] shared</code> <code>{group partition}</code>	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.

cgenv6 template dns

Description Configure a DNS template to enable DNS64 and set DNS64 options.

Syntax `[no] cgenv6 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
<pre>[no] class-list class-list lid num {conn- rate-limit over- limit- action}</pre>	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.
<pre>[no] default- policy [nocache cache]</pre>	Specify the default action to take when a query does not match any class-list entries.
<pre>[no] disable-</pre>	Disables the DNS template.

Command	Description
<code>dns-template</code>	
<code>[no] dns-log-enable</code> <code>period</code> <code>period</code>	Specify how often log messages are generated for DNS caching. (1-10000 minutes)
<code>[no] dns64</code>	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 <code>dns64</code> 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 <code>dns64</code> 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 <code>dns64</code> option is enabled, this sub-option is disabled. 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.

Command	Description
	• 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 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 <i>num</i> Forwards the response from the

Command	Description
	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 <code>dns64</code> option is enabled, this value is set to 128 by default. • <code>parallel-query</code> 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 <code>dns64</code> option is enabled, this sub-option is disabled. NOTE: It is recommended to disable passive queries (<code>passive-query disable</code>) and the single-response option enabled (no single response-disable) when using the <code>parallel-query</code> option. • <code>passive-query-disable</code> Initiates an A query upon receiving an empty response or error for a AAAA query. When the <code>dns64</code> option is enabled, this sub-option is enabled. • <code>retry retry-num</code> 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 <code>dns64</code> option is enabled, this value is set to 3 by default.

Command	Description
	• 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 <i>seconds</i> 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 IPv6 address. When the dns64 option is enabled, this sub-option is disabled. • ttl <i>seconds</i> Specifies the maximum TTL to use in

Command	Description
	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

cgmv6 dns64-virtualserver

Description Configure the virtual server for the DNS proxy, to which clients will send DNS queries.

Syntax `[no] cgmv6 dns64-virtualservername {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
<code>[no] port</code> <code>port-number</code> <code>dns-udp</code>	Specifies the UDP port number and the port type, <code>dns-udp</code>. This command changes the CLI to the configuration level for the port, where the following commands are available: • <code>service-group group-name</code> Binds the virtual port to the service group. • <code>source-nat {auto pool}</code> Binds the virtual port on an IP NAT pool or pool group. Use the <code>auto</code> option to configure auto NAT for the vport. Use the <code>pool</code> option to specify NAT pool or pool group. • <code>template dns template-name</code> Binds the virtual port to the DNS template containing the DNS64 settings. • <code>template policy template-name</code> Binds the virtual port to a policy template, if

Command	Description
	applicable. • enable enables the virtual port • disable disables the virtual port.
[no] template policy <i>template-</i> <i>name</i>	Binds a policy template to the virtual server, if applicable.
[no] vrid <i>vrid</i>	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
<i>list-name</i>	Adds the list to the running-config.
<i>filename</i> 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
<code>[no] ipv6-addr/prefix {glid lid lsn-lid} num</code>	Adds an entry to the class list. <i>ipv6-addr/prefix</i> - Specifies an IPv6 address or prefix on which to perform an override action <i>{glid lid} num</i> - Specifies a Global Limit ID (GLID) or a Limit ID (LID) configured in a policy template. These options apply only to NAT64 override. <i>lsn-lid num</i> - 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
<code>[no] dns64 {disable exclusive- answer prefix ipv6- addr/nn}</code>	Specifies the override action: • 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. • 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.

Command	Description
	• prefix <i>ipv6-addr/nn</i> – 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

cgenv6 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:

- [cgenv6 nat pool](#)

cgenv6 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:

- [cgenv6 nat pool-group](#)

cgenv6 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 [cgenv6 template policy](#).

Syntax `[no] cgenv6 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
<code>[no] source-nat-pool pool-name</code>	Binds an IPv4 NAT pool to the LID.
<code>[no] user-quota-prefix-length mask-length</code>	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: • <code>trans-eprt-to-port</code> – EPRT (RFC 2428) to PORT • <code>trans-epsv-to-pasv</code> – EPSV (RFC 2428) to PASV

Parameter	Description
	• <code>trans-lprt-to-port</code> – LPRT (RFC 1639) to PORT • <code>trans-lpsv-to-pasv</code> – LPSV (RFC 1639) to PASV • <code>xlat-no-trans-pasv</code> – Skip PASV response. The Payload of the IP address information will not be translated from IPv4 to IPv6
<code>h323</code> { <code>enable</code> <code>disable</code> }	Enables or disables NAT64 ALG support for H323 standard.
<code>mgcp</code> { <code>enable</code> <code>disable</code> }	Enables or disables NAT64 ALG support for Media Gateway Control Protocol (MGCP).
<code>pptp</code> { <code>enable</code> <code>disable</code> }	Enables or disables NAT64 ALG support for Point-to-Point Tunneling Protocol (PPTP).
<code>rtsp</code> { <code>enable</code> <code>disable</code> }	Enables or disables NAT64 ALG support for Real Time Streaming Protocol (RTSP).
<code>sip</code> { <code>enable</code> <code>disable</code> }	Enables or disables NAT64 ALG support for Session Initiation Protocol (SIP).
<code>tftp</code> { <code>enable</code> <code>disable</code> }	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

`cgnav6 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	<code>cgnav6 nat64 force-non-zero-ipv4-id [all]</code>
	The <code>all</code> 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 <code>all</code> 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.

cgnav6 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	<code>[no] cgnav6 nat64 fragmentation df-bit-transparency enable</code>
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.

cgnav6 nat64 fragmentation inbound

Description	Configure fragmentation support for inbound packets.
Syntax	<code>[no] cgnav6 nat64 fragmentation inbound {df-set drop ipv6}</code>

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.

cgnav6 nat64 fragmentation inbound df-set

Description Configure the behavior for inbound fragmented packets when Don't Fragment (DF) bit is set.

Syntax

```
[no] cgnav6 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.

Parameter	Description
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

cgnav6 nat64 fragmentation outbound

Description Configure fragmentation support for outbound packets.

Syntax

```
[no] cgnav6 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

cgnav6 nat64 icmp

Description Send ICMP Destination Unreachable messages when there are no protocol ports available for NAT mappings, or when 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 <i>n</i>	Changes the MSS to the length you specify.
none	Does not change the MSS value.
subtract <i>s</i> [<i>min</i> <i>n</i>]	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 <i>S</i> is greater than <i>N</i>, subtract <i>S</i> from the MSS. • If MSS minus <i>S</i> is less than or equal to <i>N</i>, set the MSS to <i>N</i>. The subtract method of MSS clamping is used by default, with the following values: <i>S</i> = 20 bytes <i>N</i> = 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

cgnav6 nat64 tcp reset-on-error

Description Send TCP resets to clients in response to invalid TCP packets from the inside network.

Syntax `[no] cgnav6 nat64 tcp reset-on-error outbound disable`

Default Enabled

Mode Configuration mode

cgnav6 nat64 user-quota-prefix-length

Description Assign a user quota to all users of a specific NAT64 prefix.

Syntax `[no] cgnav6 nat64 user-quota-prefix-length mask-length`

Parameter	Description
<i>mask-length</i>	Prefix length, 1-128.

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 cgnav6 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.

cgnav6 template policy

Description Configure a policy template, to override the configured NAT64 behavior for specific IPv6 addresses or prefixes.

Syntax `[no] cgnav6 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
<code>[no]</code> class-list <i>list-name</i>	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 13-dest - Extract the client's IP address from the Layer 7 header, using the destination IP as the client's IP address. ◦ client-ip 17-header [<i>L7-header-name</i>] – 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 <i>ipv6-addr/nn</i> 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

Command	Description
	DNS request. The client's request is forwarded to the DNS server, and the reply is sent to client without modification. prefix <i>ipv6-addr/nn</i> – 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 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	<code>[no] ip nat-global reset-idle-tcp-conn</code>
Default	Disabled
Mode	Configuration mode

ip frag timeout

Description	Configures IP fragmentation parameters.
Syntax	<code>{ip ipv6} frag timeout <i>millisecond</i></code>
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	Configure the maximum number of pending reassembly sessions allowed.
Syntax	<code>ip frag max-reassembly-sessions <i>num</i></code>
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
<i>list-name</i>	Adds the list to the running-config.
<i>filename file</i>	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
<code>[no]</code> <code>ipv6-</code> <code>addr</code> <code>/prefix-</code> <code>length</code> <code>lsn-lid</code> <code>num</code>	Adds an entry to the class list. <code>ipv6-addr/prefix-length</code> – Specifies the range of client IPv6 addresses on which to match. These are the IPv6 addresses of the customer DS-Lite routers. <code>lsn-lid num</code> – 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.

cgenv6 ds-lite alg

Description Configure Application Level Gateway (ALG) support for DS-Lite.

Syntax

```
[no] cgenv6 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

cgenv6 ds-lite fragmentation inbound

Description Configure fragmentation support for inbound packets.

Syntax

```
[no] cgenv6 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

cgenv6 ds-lite fragmentation outbound

Description Configure fragmentation support for outbound packets.

Syntax

```
[no] cgenv6 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 <code>df-set</code> option disallows override of the Don't Fragment bit.
[df-set] ipv4	Enables fragmentation support for outbound IPv4 packets. The <code>df-set</code> 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 <code>df-set</code> 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

cgenv6 ds-lite icmp

Description Send ICMP Destination Unreachable messages when there are no protocol ports available for NAT mappings, or when a user quota is exceeded.

Syntax

```
[no] cgenv6 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-quota-exceeded	Sends ICMP Destination Unreachable message when a user quota is exceeded.

Parameter	Description
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

cgnav6 ds-lite inside source class-list

Description Bind a class list for use with DS-Lite.

Syntax `[no] cgnav6 ds-lite inside source class-list list-name`

Replace *list-name* with the name of the class list.

Default None

Mode Configuration mode

cgnav6 ds-lite ip-checksum-error

Description Configure handling of IP checksum errors in DS-Lite tunneled IP traffic.

Syntax `[no] cgnav6 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.

cgenv6 ds-lite l4-checksum-error

- Description** Configure handling of Layer 4 checksum errors in DS-Lite tunneled IP traffic.
- Syntax** `[no] cgenv6 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.

cgenv6 ds-lite port-reservation

- Description** Configure static mappings for a range of protocol ports for an IPv4 address

Syntax `[no] cgenv6 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
<i>ipv6-tunnel-source</i>	Inside client's tunnel source IPv6 address.
<i>ipv6-tunnel-destination</i>	Inside client's tunnel destination IPv6 address.
<i>ipv4-inside-addr</i>	Client IPv4 address.
<i>inside-start-</i>	Beginning Layer 4 protocol port number in the

Parameter	Description
<i>portnum</i>	port range to be mapped.
<i>inside-end-port</i>	Ending Layer 4 protocol port number in the port range to be mapped.
nat <i>nat-ipaddr</i>	Public IPv4 address to map to the client IPv4 address.
<i>nat-start-portnum</i>	Beginning Layer 4 protocol port number to map to the inside port range.
<i>nat-end-portnum</i>	Ending Layer 4 protocol port number to map to the inside port range.

Default None

Mode Configuration mode

cgenv6 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] cgenv6 ds-lite tcp mss-clamp
{fixed n | none | subtract s [min n]}
```

Parameter	Description
fixed <i>n</i>	Changes the MSS to the length you specify.
none	Does not change the MSS value.
subtract <i>s</i> [min <i>n</i>]	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. The subtract method of MSS clamping is used by

Parameter	Description
	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

cgnav6 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] cgnav6 ds-lite tcp reset-on-error outbound disable`

Default Enabled

Mode Configuration mode

cgnav6 ds-lite user-quota-prefix-length

Description Assign a user quota to all users of a specific DS-Lite prefix.

Syntax `[no] cgnav6 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	<pre>[no] cgnv6 pcp default-template <i>template-name</i></pre> Replace <i>template-name</i> 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 <code>cgnv6 pcp default-template</code> 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
<code>[no] allow-third-party-from-lan</code>	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.
<code>[no] allow-third-party-from-wan</code>	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.
<code>[no] check-client-nonce</code>	Enable validation of the PCP MAP NONCE. By default, this option is disabled.
<code>[no] disable-map-filter</code>	Disable the process to FILTER in PCP MAP. By default, this option is enabled.
<code>[no] disable-</code>	Enable or disable the process for

Command	Description
opcode <i>option</i>	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 <i>portnum</i>	Specifies the UDP destination port for PCP, 1024-65535. The default is 5351.
[no] send-unsolicited-announce { source-ip <i>ipv4addr</i> source-ipv6 <i>ipv6addr</i> }	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 **cgnav6 pcp default-template** command to activate it ([cgnav6 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
<code>[no] batched-logging-disable</code>	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.
<code>[no] custom options</code>	Configures custom LSN log strings. • <code>custom header use-syslog-header</code> – Adds a syslog header to each message. (Disabled by default. By default, no header is included.) • <code>custom message <i>type string</i></code> – Customizes a logging string. The <i>type</i> can be one of the following: ◦ <code>fixed-nat-allocated</code> ◦ <code>fixed-nat-freed</code> ◦ <code>fixed-nat-interim-update</code>

Command	Description
	○ <code>http-request-got</code> ○ <code>port-allocated</code> ○ <code>port-batch-allocated</code> ○ <code>port-batch-freed</code> ○ <code>port-batch-v2-allocated</code> ○ <code>port-batch-v2-freed</code> ○ <code>port-batch-v2-interim-update</code> ○ <code>port-freed</code> ○ <code>session-created</code> ○ <code>session-deleted</code> ○ <code>message-string</code> - 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. ● <code>customtime-stamp-format</code> - Customizes the time stamp format to use in the message strings. The default format is <code><%Y><%m><%d><%H%M%S></code>, where <code><%m></code> displays the month numerically. You can also set the time stamp format as <code>"<%Y><%o> <%d> <%H:%M:%S>"</code>, where <code><%o></code> 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.
<code>[no] disable-log-by-destination</code>	Disables logging by specific protocol and destination port/range of ports. The following options are available: • <code>icmp</code> – disables logging for ICMP traffic • <code>ip</code> – configures a filter for IP entry • <code>ip6</code> – configures a filter for IPv6 entry • <code>others</code> – disables logging for other protocols • <code>tcp</code> – disables logging by destination TCP port • <code>udp</code> – disables logging by destination UDP port
<code>[no] enable-log-by-destination</code>	Enables logging by specific protocol, destination IP address, port, and range of ports. The following options are available: • <code>icmp</code> – enables logging for ICMP traffic • <code>ip</code> – configures a filter for IP entry • <code>ip6</code> – configures a filter for IPv6 entry • <code>others</code> – enables logging for other protocols • <code>tcp</code> – enables logging by destination TCP port • <code>udp</code> – enables logging by destination UDP port
<code>[no] facility facility-name</code>	Specifies the logging facility to use. For a list of available facilities, enter the following command: facility ?
<code>[no] format option</code>	Reduces the size of external traffic logs. You can enable one of the following data reduction options: • <code>binary</code> – Uses a unique A10 Binary Logging format to represent the log messages. • <code>compact</code> – 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.
<code>[no] include-destination</code>	Includes the destination IP addresses and protocol ports in NAT port mapping logs.
<code>[no] include-httpoption</code>	Includes additional HTTP information in the log messages. • cookie <code>[max-length num]</code> – Includes cookie information. • file-extension – Includes HTTP file extension. • 14-session-info – Includes TCP session information. • method – Includes the HTTP method; for example: GET or POST. • referer <code>[max-length num]</code> – Includes the information in the Referer header.

Command	Description
	• request-number – Includes the HTTP request number. • user-agent [max-length <i>num</i>] – Includes the information in the User-Agent header. • header1 [max-length <i>num</i>], header2 [max-length <i>num</i>], header3 [max-length <i>num</i>] – 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 <i>option</i>	Enables logging for specific options. • fixed-nat <pre>{ http-requests {host url} port-mappings {both creation} sessions user-ports [periodic days start-time hh:mm] }</pre>

Command	Description
	Enables logging for Fixed-NAT. • <code>http-requests {host url}</code> Enables logging of information from HTTP requests. NOTE: The maximum length of the <code>log http-requests host</code> option is 255. • <code>port-mappings {both creation}</code> Logs Fixed-NAT port mappings. Use <code>both</code> to log both creation and deletion of NAT mappings; use <code>creation</code> to log creation of NAT mappings only. • <code>sessions [merged-style]</code> Logs Fixed-NAT session creation and deletion. The <code>merged-style</code> option merges creation and deletion of session logs to one. • <code>user-ports [periodic days start-time hh:mm]</code> Includes the port numbers assigned to clients. The <code>periodic</code> option specifies the Interval between log generation for Fixed-NAT port allocations. You can specify 1-30 days. The <code>start-time</code> option specifies the time at which to generate the first user activity log. This is the local system time on the ACOS device. • <code>http-requests {host url}</code> Enables logging of information from HTTP requests. • <code>host</code> logs the hostname requested by the client. • <code>url</code> 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: <i>YYYY MMM DD HH:MM:SS</i> Enabling this option disables use of timestamps formatted in compliance with RFC 5424, The Syslog Protocol.
[no] rfc-custom-message <i>feature type string</i>	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" • 1sn – 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 1sn and nat64. The <i>string</i> 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.)
<pre>[no] rule http- requests option</pre>	Configures rules for HTTP request logging. You can set the following options: • dest-port <i>portnum</i> [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 <i>max-number-of-characters</i> – 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 <i>ipv4addr</i> ipv6 <i>ipv6addr</i> }	Specifies the source IPv4 or IPv6 address to use as the source of log packets.
[no] source-port { <i>portnum</i> 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
<code>\$rule-name\$</code>	Rule used in the session.
<code>\$proto-name\$</code>	Protocol used in the session.
<code>\$proto-</code>	Protocol number used in the session.

Keyword	Description
num\$	
\$fwd-tuple-type\$	Forward tuple type used in the session.
\$fwd-tunnel\$	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-tunnel\$	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-tunnel\$	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-tunnel\$	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-tunnel\$	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-tunnel\$	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-tunnel\$	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
<code>src-port\$</code>	
<code>\$rev-dst-tunnel\$</code>	Reverse tuple destination tunnel used in the session.
<code>\$rev-dst-ip\$</code>	Reverse tuple destination IP address of the session.
<code>\$rev-dst-port\$</code>	Reverse tuple destination port number of the session.
<code>\$req-byte\$</code>	Request byte count of the session.
<code>\$rsp-byte\$</code>	Response byte count of the session.
<code>\$sesn-dur\$</code>	Duration of the session.
<code>\$sesn-fwd-byte\$</code>	Forward byte count of the session.
<code>\$sesn-rev-byte\$</code>	Reverse byte count of the session.
<code>\$sesn-start-time\$</code>	Start time of the session.
<code>\$sesn-start-time-epoch\$</code>	Epoch start time of the session.
<code>\$sesn-end-time\$</code>	End time of the session.

Keyword	Description
<code>\$sesn-end-time-epoch\$</code>	Epoch end time of the session.
<code>\$radius-msisdn\$</code>	RADIUS attribute: MSISDN
<code>\$radius-imei\$</code>	RADIUS attribute: IMEI
<code>\$radius-imsi\$</code>	RADIUS attribute: IMSI
<code>\$radius-ctm1\$</code>	RADIUS attribute: Custom1
<code>\$radius-ctm2\$</code>	RADIUS attribute: Custom2
<code>\$radius-ctm3\$</code>	RADIUS attribute: Custom3
<code>\$radius-ctm4\$</code>	RADIUS attribute: Custom4
<code>\$radius-ctm5\$</code>	RADIUS attribute: Custom5
<code>\$radius-ctm6\$</code>	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
```

cgnav6 server

Description Configure a server for external logging.

Syntax `[no] cgnav6 server server-name ipaddr`

Parameter	Description
<i>server-name</i>	Server name, 1-31 characters.
<i>ipaddr</i>	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.
<code>[no] health-check [monitor-name]</code>	Enables health monitoring of the server. The <i>monitor-name</i> specifies the name of a configured health monitor. If you omit this command or you enter it without the <i>monitor-name</i> option, the default Layer 3 (ICMP) health monitor is used.
<code>[no] health-check-disable</code>	Disables health monitoring of the server.
<code>[no] health-check-follow-port portnum {tcp udp}</code>	Specifies the specific port to follow for health status.
<code>[no] port port-num {tcp udp}</code>	Specifies the TCP or UDP port on which the server listens for log traffic. disable enable Disables or re-enables the port.

Command	Description
	<code>[no] health-check [monitor-name]</code> Enables health monitoring of the port. The <code>monitor-name</code> option specifies the name of a configured health monitor. If you omit the <code>health-check</code> command or you enter it without the <code>monitor-name</code> option, the default UDP health monitor is used. <code>[no] health-check-disable</code> Disables health monitoring of the port.

Default There is no default logging server configuration.

Mode Configuration mode

Usage The normal form of the `cnv6 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.

cgnav6 service-group

Description Configure a service group, which is a pool of one or more servers.

Syntax `[no] cgnav6 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
<code>[no] health-check</code> <code>[monitor-name]</code>	Enables health monitoring of the service group. The monitor-name specifies the name of a configured health monitor.
<code>[no] member</code> <code>server-name</code> <code>portnum</code>	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.

cgenv6 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] cgenv6 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)# cgenv6 ecmp 4-tuple-hash
```

cgenv6 lsn alg

Description Disables or re-enables Application Level Gateway (ALG) support for LSN and Fixed-NAT.

Syntax `[no] cgenv6 lsn alg
{dns | esp | ftp | h323 | mgcp | pptp | rtp-stun-timeout | rtsp
| sip | tftp}
{enable | disable}`

Parameter	Description
<code>dns</code>	Disables ALG support for Domain Name System (DNS).
<code>esp</code>	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

cgenv6 fixed-nat create-port-mapping-file

Description Creates a port mapping file.

Syntax `[no] cgenv6 fixed-nat create-port-mapping-file`

Default Not set

Mode Configuration mode

Example The following is an example of the command

```
ACOS(config)# cgenv6 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
<i>options</i>	To specify a single range: • <i>start-inside-ipaddr</i> – Beginning (lowest-numbered) inside client address. • <i>end-inside-ipaddr</i> – Ending (highest-numbered) inside client address. • netmask – Network mask, in the applicable format: ◦ IPv4 – <i>/mask-length</i> or <i>ipaddr</i> ◦ IPv6 – <i>mask-length</i>
nat <i>options</i>	To specify a single range: • <i>start-nat-ipaddr</i> – Beginning (lowest-numbered) NAT address. • <i>end-nat-ipaddr</i> – Ending (highest-numbered) NAT address. To specify multiple ranges: • ip-list <i>list-name</i> – Name of a configured IP list.
partition <i>options</i>	Configures settings for inside user partition.
dest-rule-list <i>name</i>	Binds destination-based rule-list.
dynamic-pool-size <i>num</i>	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 <i>offset-</i> <i>value</i> }	Allocation offset. (For more information, see the IPv6 Migration Logging Guide.)
ports-per- user <i>num</i>	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 <i>quota-num</i>	Maximum number of sessions that can be created for a given client. You can specify 1-2147483647.
usable- nat-ports <i>starting-</i> <i>port</i> <i>ending-</i> <i>port</i>	Range of protocol ports that can be allocated to clients. You can specify 1024-65535.
vrid <i>vrid</i>	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.

cgenv6 nat46-stateless fragmentation inbound

Description Change fragmentation support for inbound IPv6-to-IPv4 traffic.

Syntax `[no] cgenv6 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

cgenv6 nat46-stateless fragmentation outbound

Description Change fragmentation support for outbound IPv4-to-IPv6 traffic.

Syntax `[no] cgenv6 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.

cgnav6 nat46-stateless static-dest-mapping

Description Configure static IPv4-IPv6 mappings for the IPv6 servers.

Syntax

```
[no] cgnav6 nat46-stateless static-dest-mapping ipv4addr
ipv6addr
[count num]
[shared | to-shared]
[vrid vrid]
```

Parameter	Description
<i>ipv4addr</i>	IPv4 server address to which IPv4 clients will send requests.
<i>ipv6addr</i>	Server's IPv6 address. Specify the lowest address in the range.
count <i>num</i>	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 through the shared partition.
vrid <i>vrid</i>	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 than 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

cgenv6 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] cgenv6 nat46-stateless tcp mss-clamp {none | fixed n | subtract s [min n] }`

Parameter	Description
fixed <i>n</i>	The fixed MSS value that you specify. The value can be 0 to 1420.
none	Does not change the MSS value.
subtract <i>s</i> [min <i>n</i>]	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 <i>S</i> is greater than <i>N</i>, subtract <i>S</i> from the MSS. • If MSS minus <i>S</i> is less than or equal to <i>N</i>, set the MSS to <i>N</i>. 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:

$$\text{MSS Minimum} = \text{IP Header maximum} - \text{TCP Header maximum (TCP\_MSS\_MTU\_MIN - TCP\_MSS\_IPH\_MAX - TCP\_MSS\_TCPPH\_MAX)}.$$

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
<i>list-name</i>	Adds the list to the running-config.
<i>filename file</i>	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

cgnav6 lw-4o6 binding-table

Description Configures a Lightweight 4over6 binding table directly on the ACOS device

Syntax `[no] cgnav6 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
<code>[no] tunnel- address <i>ipv6- address</i></code>	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: <code>[no]nat-address <i>ipv4-address</i></code> – 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: <code>port <i>num</i> [<i>tonum</i>]</code> – Specifies the port range for the NAT address in the binding table entry. The <code>tunnel-endpoint-address</code> option is available to configure LW-4o6 IPIP Tunnel Endpoint Address. Using the “no” form of either the <code>nat-address</code> or <code>tunnel-address</code> 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
<code>df-set {drop ipv4 ipv6 </code>	The <code>df-set</code> 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

cgnav6 lw-4o6 fragmentation outbound

Description Configures fragmentation support for outbound packets.

Syntax

```
[no] cgnav6 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

cgnav6 lw-4o6 hairpinning

Description Configures hairpinning for Lightweight 4over6 clients.

Syntax

```
[no] cgnav6 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.

cgenv6 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] cgenv6 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)# cgenv6 lw-4o6 health-check-gateway 9.9.9.173
```

```
ACOS(config)# cgenv6 lw-4o6 health-check-gateway 3201::172
```

NOTE: This command can only be configured on the shared partition.

cgenv6 lw-4o6 icmp-inbound

Description Configures handling of inbound IPv4 ICMP traffic for Lightweight 4over6 traffic. This applies to IPv4 traffic from the Internet for sessions using Lightweight 4over6 bindings.**Syntax** `[no] cgenv6 lw-4o6 icmp-inbound {drop | handle}`

Parameter	Description
<code>drop</code>	Drops inbound ICMP traffic.
<code>handle</code>	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	<code>[no] cgnv6 lw-4o6 inside-src-access-list <i>acl-num</i></code>
Default	None
Mode	Configuration mode
Usage	The feature applies an ACL to Lightweight 4over6 traffic.
NOTE:	The <i>acl-num</i> 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	<code>[no] cgnv6 lw-4o6 nat-prefix-list <i>class-list-name</i></code>
Example	The following example applies a class-list named “v-4o6” as the NAT Prefix List for Lightweight 4over6. <pre>ACOS(config) # cgnv6 lw-4o6 nat-prefix-list v-4o6</pre>
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	<code>[no] cgnv6 lw-4o6 no-forward-match send-icmpv6</code>

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	<code>[no] cgnv6 lw-4o6 no-reverse-match send-icmp</code>
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 btl
```

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 <i>rule-name</i> 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 <i>domain-name</i>	Create a description for the MAP-T domain

Parameter	Description
<code>format {draft-03}</code>	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.
<code>health-check-gateway {ipv4-addr ipv6-addr withdraw-route}</code>	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)
<code>tunnel-endpoint-address {ipv6-addr}</code>	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.

cgenv6 map encapsulation fragmentation inbound

Description Configures fragmentation support for inbound packets sent to the CPE.

Syntax

```
[no] cgenv6 map encapsulation fragmentation inbound
{df-set | drop | ipv4 | ipv6}
send-icmp
```

Parameter	Description
<code>df-set {drop ipv4 ipv6 send-icmp}</code>	The <code>df-set</code> option handles packet when df-bit is set in the IPv4 header. The <code>send-icmp</code> 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

cgnav6 map encapsulation fragmentation outbound

Description Configures fragmentation support for outbound packets sent to the server.

Syntax

```
[no] cgnav6 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

cgenv6 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] cgenv6 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 <i>rule-name</i> 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 <i>ipv6-prefix</i> }	Configure the default mapping rule (DMR) to map IPv4 addresses to IPv6 addresses beyond the MAP-T domain.
description <i>domain-name</i>	Create a description for the MAP-T domain
health-check-gateway { <i>ipv4-addr</i> <i>ipv6-addr</i> 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 <i>num</i>	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.

cgenv6 map translation fragmentation inbound

Description Configures the action to be taken when inbound IPv4 packets are too large.

Syntax `[no] cgenv6 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.

cgenv6 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] cgenv6 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.

cgenv6 map translation fragmentation outbound

Description Configures the action to be taken when an outbound IPv6 packet is too large.

Syntax

```
[no] cgenv6 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

cgnav6 nptv6 domain

Description Configures NPTv6 translation to manage network traffic.

Syntax `[no] cgnav6 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 <i>ipv6addr</i>	This command specifies the inside-prefix for an NPTv6 domain.
outside-prefix <i>ipv6addr</i>	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.

cgnav6 nptv6 common send-icmpv6-on-error disable

Description Disable error notifications on NPTv6 translation failure.

Syntax	<code>cgnv6 nptv6 common send-icmpv6-on-error disable</code>
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.

cgenv6 sixrd domain

Description Configure 6rd domain settings.

Syntax `[no] cgenv6 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
<code>[no] br- ipv4- address <i>ipv4addr</i> ipv6-prefix <i>ipv6addr</i> <i>/prefix- length</i></code>	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 <i>ipv4addr</i> { <i>subnet-mask</i> <i>/mask-length</i> }	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 <i>bytes</i>	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.

cgenv6 sixrd fragmentation inbound

Description Configure fragmentation support for oversize inbound IPv6 packets. These are packets from IPv6 servers to 6rd clients.

Syntax

```
[no] cgenv6 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.

cgenv6 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] cgenv6 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 <code>send-icmp</code> .
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	<code>[no] acos-application-only</code>
Mode	BGP neighbour level
Usage	After configuring a neighboring BGP router, route updates from this neighboring router is treated specially using the <code>acos-application-only</code> 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	<code>[no] cgnv6 ddos-protection {disable enable}</code>
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	<code>[no] cgnv6 ddos-protection disable-nat-ip-by-bgp zone <i>name</i></code>
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	<code>[no] cgnv6 ddos-protection logging {disable enable}</code>
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	<code>[no] cgnv6 ddos-protection max-hw-entries <i>number</i></code>
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
<code>include-existing-session</code>	Count traffic associated with an existing session into the packets-per-second. The default is disabled.
<code>ip other tcp </code>	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.
<i>num</i>	Maximum number of packets per second allowed. The maximum configurable limit is 30000000 packets.
action {log drop} expiration <i>seconds</i>	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 <i>route-map-name</i> } expiration <i>seconds</i> remove-wait-timer <i>seconds</i> timer- multiply-max <i>num</i> 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 <i>route-map-name</i> 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 <code>log</code> and <code>drop</code> 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.
<i>threshold</i>	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
<code>on-threshold</code> <code><num></code>	The threshold for TCP half-open sessions. SYN cookie protection is enabled after the specified threshold exceeds.
<code>on-timeout</code> <code><num></code>	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
<code>[no] conn-rate-limit num</code>	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 <i>num1</i> [to <i>num2</i>]]	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 (<i>num1</i>) for the Option Type in the EH or you can specify a range (<i>num1</i> to <i>num2</i>) 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 <i>num1</i> [to <i>num2</i>]]	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 (<i>num1</i>) for the Option Type in the EH or you can specify a range (<i>num1</i> to <i>num2</i>) 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 <i>num1</i> [to <i>num2</i>]]	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 (<i>num1</i>) for the Routing Type in the EH or you can specify a range (<i>num1</i> to <i>num2</i>) 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 <i>num1</i> [to <i>num2</i>]	Specify this option to drop all packets that contain an unknown Extension Header type. You can specify a particular value (<i>num1</i>) or specify a range (<i>num1</i> to <i>num2</i>) 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 FPGA 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	<code>clear cgnv6 ddos-protection disabled-ip-by-bgp {all ip-address <i>ip-addr</i>}</code>
Mode	Configuration mode

clear cgnv6 ddos-protection ip-entries

Description	Clear DDoS IP entries.
Syntax	<code>clear cgnv6 ddos-protection ip-entries {all ip-address <i>ip-addr</i> nat-pool <i>name</i>}</code>
Mode	Configuration mode

clear cgnv6 ddos-protection l4-entries

Description	Clear DDoS L4 entries.
Syntax	<code>clear cgnv6 ddos-protection l4-entries {address <i>ipaddr</i> all l4-proto <i>protocol-num</i> nat-pool <i>name</i> port <i>port-num</i>}</code>
Mode	Configuration mode

clear cgnv6 ddos-protection statistics

Description	Clear DDoS statistics.
Syntax	<code>clear cgnv6 ddos-protection statistics</code>
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
      NAT Address      Conns  Pool      Inside Address
                        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
<i>nataddr</i>	Specifies the NAT IP address.
<i>natport</i>	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 <i>pool-name</i>	Shows currently active full-cone sessions only for the specified pool. If you omit this option, sessions for all pools are shown.
top num <i>type</i>	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 <i>name</i>	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
<i>portnum</i>	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 administratively 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
<i>feature</i>	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.
<i>event</i>	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")
$radius-msisdns$           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	<code>show cgnv6 logging source-address</code>
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	<code>show cgnv6 logging statistics</code>
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 template template-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: <i>Established-Connections / Data-CPU</i>s 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-CPU 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-user ipaddr]
[partition partition-name]
[pool pool-name]
```

Parameter	Description
all-partitions partition <i>partition-name</i>	Displays session information for all partitions or for a particular partition.
inside-user <i>ipaddr</i>	Displays session information only for the specified user IP address.
pool <i>pool-name</i>	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           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 <i>partition-name</i>	Displays full-cone sessions for all partitions or for a particular partition.
inside-user	Displays full-cone sessions only for the specified

Parameter	Description
<i>ipaddr</i>	user.
pcp	Displays full-cone sessions created by PCP requests.
pool <i>pool-name</i>	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-address nataddr [nat-port natport]`

Parameter	Description
<i>nataddr</i>	Specifies the NAT IP address.
<i>natport</i>	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 tcp disable 1 to 79
cgnv6 lsn port-overloading tcp enable 80
cgnv6 lsn port-overloading tcp disable 81 to 65535
cgnv6 lsn port-overloading udp disable

LSN Port-Overloading Actual:
cgnv6 lsn port-overloading tcp disable 1 to 79
cgnv6 lsn port-overloading tcp enable 80
cgnv6 lsn port-overloading tcp disable 81 to 65535
cgnv6 lsn port-overloading udp disable
```

NOTE: For Thunder 14045 devices, the output is displayed only for Master. For Thunder 7650 devices, the output is displayed only for one instance of the processing unit.

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	Total number of ICMP ports freed for use by other

Field	Description
Ports Freed	sessions.
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.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
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.
Port Overloading 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.

Field	Description
HA NAT Pool Unusable	Number of times traffic hit a disabled NAT IP in high availability standby state.
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 Status	Shows memory usage information.
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-user ipaddr]
[partition partition-name]
[pool pool-name]
[topnum {all | icmp | tcp | udp}]
```

Parameter	Description
all-partitions partition <i>partition-name</i>	Displays session information for all partitions or for a particular partition.
inside-user <i>ipaddr</i>	Displays session information only for the specified user IP address.
pool <i>pool-name</i>	Displays session information only for the specified LSN NAT pool.

Parameter	Description
top <i>num type</i>	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 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.

Field	Description
UDP	Number of UDP ports from the quota that are in use.
TCP	Number of TCP ports from the quota that are in use.
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
<i>list-name</i>	Displays information for the specified CGN rule list.
<i>domain-ip</i>	Displays IPs for domain. For each rule in the list, the number of times traffic matched the rule (the number

Parameter	Description
	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 dn timer 1.000000 hits 0 domain-
unresolved-drops 0
    icmp action dn timer 1.000000 hits 2 domain-unresolved-
drops 0
ip 7.7.7.104/32
    tcp port 0 action dn timer 1.000000 hits 0 domain-
unresolved-drops 0
    icmp action dn timer 1.000000 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 dn timer 1.000000 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 <i>ipv6addr</i> [entries]	Displays information for the specified Lightweight 4over6 tunnel address.

Mode All

NOTE: For Thunder 14045 devices, the output is displayed only for Master. For Thunder 7650 devices, the output is displayed only for one instance of the processing unit.

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
```

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>
```

NOTE: For Thunder 14045 devices, the output is displayed only for Master. For Thunder 7650 devices, the output is displayed only for one instance of the processing unit.

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 Display the configured NAT pools.

Syntax `show cgnv6 nat pool statistics[options] [pool-name]`

Parameter	Description
<i>pool-name</i>	Displays statistics for the specified CGN pool.
statistics <i>[options]</i>	Displays CGN pool statistics. The following filtering options are available: • <i>pool-name</i> – 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. ◦ used-udp – Displays the pool IP addresses with the highest UDP port usage.

Parameter	Description
	◦ 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.

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.

Field	Description
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
0	1	1	0	0	0				
19.19.19.110	1	0	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.
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	Total number of TCP ports freed.

Field	Description
(TCP)	
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_pl	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_pl	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

show cgnv6 nat pool-group

Description Display the configured NAT pool groups.

Syntax `show cgnv6 nat pool-group group-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	Number of outbound IPv6 packets fragmented.

Field	Description
fragmented	
Inbound IPv6 packets received	Number of inbound IPv6 packets received.
Inbound IPv6 packets dropped	Number of inbound IPv6 packets dropped.
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 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
<i>ipv4-addr</i> <i>ipv6-addr</i>	Specifies the IP address to convert. • <i>ipv4-addr</i> – To display the IPv6 version of an IPv4 address, enter the IPv4 address. • <i>ipv6-addr</i> – To display the IPv4 version of an IPv6 address, enter the IPv4 address.
prefix <i>NAT64-prefix</i>	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-user ipaddr]
[partition partition-name]
[pool pool-name]
```

Parameter	Description
all-partitions	Displays session information for all partitions

Parameter	Description
<i>partition-name</i>	or for a particular partition.
inside-user <i>ipaddr</i>	Displays session information only for the specified user IP address.
pool <i>pool-name</i>	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.

Field	Description
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 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 <i>partition-name</i>	Only show sessions from a specific partition.
pcp	Displays only the full-cone sessions that were created by a PCP request.
pool <i>pool-name</i> [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	Number of UDP full-cone sessions freed.

Field	Description
Information for Individual Sessions:	
Session 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-user ipv6addr`

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-	Lists the following user-quota session

Field	Description
Quota Sessions	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 • 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	Lists the following data session information for

Field	Description
Sessions	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 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
<i>nataddr</i>	Specifies the NAT IP address.
<i>natport</i>	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 • 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.
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.

Field	Description
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.
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.

Field	Description
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-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.

Field	Description
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.
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.

Field	Description
Layer 3 Forwarded Packets	Number of packets forwarded at Layer 3 because the IPv6 destination address did not match the NAT64 prefix.
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 <i>partition-name</i>	Show users in a specific partition.
pool <i>pool-name</i>	Displays session information only for the specified NAT pool.
prefix <i>ipv6addr/prefix-length</i>	Displays session information only for the specified IPv6 address(es).

Parameter	Description
top <i>num type</i>	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 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	Public IP address assigned to the client.

Field	Description
Address	
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.
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	Number of times the ICMP quota for a user was

Field	Description
User-Quota Exceeded	exceeded.
NAT64 Extended User-Quota Matched	Number of times the extended user quota was 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 [<i>domain-name</i>]	Display all NPTv6 domains or a specific domain.
statistics [<i>domain-name</i>]	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-address ipaddr]
[partition partition-name]
[pool pool-name [shared]]
```

Parameter	Description
all-partitions partition <i>partition-name</i>	Displays mappings for all partitions or for a particular partition.
inside-address <i>ipaddr</i>	Displays information for a specific inside address.
inside-address-	Displays information for a specific IPv6 inside address.

Parameter	Description
ipv6 <i>ipv6-addr</i>	
nat-address <i>ipaddr</i>	Displays information for a specific NAT address.
partition <i>partition-name</i>	Displays information for a specific partition.
pool <i>pool-name</i>	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.

Field	Description
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
<code>pool [pool-name]</code>	Displays the name of the pool.
<code>statistics</code>	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	Number of NAT44 PCP ANNOUNCE requests received and processed successfully by ACOS.

Field	Description
Processing Success (NAT44)	
PCP ANNOUNCE Request Processing Success (DS-Lite)	Number of DS-Lite PCP ANNOUNCE requests received and processed successfully by ACOS.
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

Field	Description
	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.
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

Field	Description
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.

Field	Description
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.
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	Number server-to-client packets fragmented into

Field	Description
Fragmented IPv6 in tunnel	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 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.

Field	Description
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.
HW Entries Invalidate due to server down	Number of hardware entries invalidated since the server was down.

Field	Description
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.

Field	Description
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.
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	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 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	Total number of TCP ports allocated for user

Field	Description
Allocated	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.
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.
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.

Field	Description
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.
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.
nat 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 Web Application Firewall (WAF) feature. The WAF filters communication between users and web applications to protect web servers and sites from unauthorized access and malicious programs. This new layer of security examines incoming user requests, output from web servers, and access to website content to safeguard against web attacks and protect sensitive information hosted on web servers.

This reference lists the CLI configuration and show commands that apply specifically to Firewall and WAF.

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
<i>rule-set-</i>	Specify the predefined rule-set to be activated.

Parameter	Description
<i>name</i>	
session-aging <i>template-name</i>	Bind the session-aging template (for TCP, UDP, and 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.

Parameter	Description
<code>esp default-port-disable</code>	Change ESP ALG settings for default port 500.
<code>esp sampling-enable</code> <i>options</i>	Enable sampling when certain events occur. You can specify one of the following events: • <code>session-created</code>: ESP sessions are created • <code>helper-created</code>: ESP helper sessions are created • <code>helper-freed</code>: ESP helper sessions freed • <code>helper-freed-used</code>: Used ESP helper sessions freed • <code>helper-freed-unused</code>: Unused ESP helper sessions freed • <code>helper-already-used</code>: ESP helper sessions already used • <code>helper-in-rml</code>: ESP helper session added to remove list • <code>all</code> : All events. So, enable sampling if any of the above-mentioned events occur.
<code>ftp default-port-disable</code>	Change FTP ALG settings for default port 21.
<code>icmp disable</code>	Disable ICMP ALG, which allows ICMP errors to pass through the firewall.
<code>pptp default-port-disable</code>	Change PPTP ALG settings for default port 1723.
<code>rtsp default-port-disable</code>	Change RTSP ALG settings for default port 554.

Parameter	Description
<code>sctp { disable enable }</code>	Disable or enable SCTP settings.
<code>sip default-port-disable</code>	Change SIP ALG settings for default port 5060.
<code>tftp default-port-disable</code>	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
<code>honor-rule-set</code>	Honor the firewall rule-set (Default)
<code>override-rule-set</code>	Override the firewall rule-set

Default	By default, <code>honor-rule-set</code> 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	<pre>[no] fw allow-non-syn-session-create</pre>
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 <code>fw tcp syn-cookie</code> 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 <code>fw allow-non-syn-session-create</code> command is enabled. To transmit non-SYN TCP packets from port 53, you need to disable the default port by executing the <code>no fw alg dns default-port-disable</code> command.
Example	The following example demonstrates the command usage: <pre>ACOS(config)# fw allow-non-syn-session-create</pre>

fw apply-changes

Description	Recompile the firewall rule-set immediately.
Syntax	<code>fw apply-changes [forced]</code>
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 zone contained within a rule, and so on. If changes are made and the command is <u>not</u> 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
<pre>action {drop redistribute-route route-map-name { expiration seconds remove-wait-timer seconds timer- multiply-max num forward }}</pre>	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 <i>route-map-name</i> 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
<code>disable]</code>	DDoS attacks by creating dynamic blacklist sessions.
<code>[inbound outbound both]</code>	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.
<code>[timeout num]</code>	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 baselining 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 a DDOS 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 cryptocurrencies, 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
<i>protocol_name</i>	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 <i><class-list-name></i>	Bind the specified string class list to an APN prefix.
log-periodicity <i><frequency></i>	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:	
<code>monitor</code>	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	<code>[no] fw gtp network-element-list-v6 <class-list-name></code>
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
<code>echo-timeout <i>timeout</i></code>	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: $\text{echo-timeout} = \text{echo interval} + 2 * T3\_resp + 4 * T3\_resp \dots (N3request-1) \text{ times}$ where, <code>echo interval</code> indicates the wait time before retransmitting the echo request after receiving the response. <code>N3 requests</code> represent the number of retries for an echo request if no response is received. <code>T3 response</code> 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.
<code>enable-log</code>	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 chassis platform. Specifying the next-hop to the specified external router ensures that the router redirects the traffic back to the appropriate Scaleout node or chassis PU 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:cg_n_zone)#dest zone any
ACOS(config-rule set:rs1-rule:cg_n_zone)#service any
ACOS(config-rule set:rs1-rule:cg_n_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
<code>idle-timeout</code>	Set the firewall helper-sessions idle-timeout to a value ranging from 1-255 minutes. Default is 1 minute.
<code>limit</code>	Limit the number of helper sessions that can be created (1-134217728).
<code>mode disable</code>	Helper sessions mode is enabled by default. You can use <code>mode disable</code> 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
<i>local-log</i>	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
<code>cef-label { enable disable }</code>	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.
<code>gtp [sampling-enable]</code>	Configure this option to include GTP counters in the logs.
<code>template-name</code>	Specify the logging template name to be bound to the firewall.
<code>sampling-enable</code>	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
<code>forward</code>	The packet will be L3 forwarded and a firewall session will be created.

Parameter	Description
<code>next-service-mode</code>	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
<code>[no] health-check [monitor-name]</code>	Enables health monitoring of the server. The <i>monitor-name</i> specifies the name of a configured health monitor. If you omit this command or you enter it without the <i>monitor-name</i> option, the default Layer 3 (ICMP) health monitor is used.
<code>[no] health-check-disable</code>	Disables health monitoring of the server.
<code>[no] port port-num {tcp udp}</code>	Specifies the TCP or UDP port on which the server listens for traffic. enable disable Enables or disables the port. <code>[no] health-check [monitor-name]</code> Enables health monitoring of the port. The <i>monitor-name</i> option specifies the name of a configured health monitor. If you omit the <code>health-check</code> command or you enter

Parameter	Description
	it without the <i>monitor-name</i> option, the default UDP health monitor is used. [no] health-check-disable Disables health monitoring of the port. [no] sampling-enable <i>type</i> 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 <i>monitor-name</i> specifies the name of a configured health monitor.
[no] member <i>server-name</i> <i>portnum</i> [sampling-enable <i>type</i>]	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 <i>seconds</i>	the timeout to a value ranging from 2-15000 seconds. The default is 2 seconds.
[no] ip-others ip-idle-timeout <i>seconds</i>	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 <i>num</i> – 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 <i>num</i> – 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 <i>num</i> – 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 <i>num</i> – 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 <i>num</i> – 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 <i>num</i> – 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 <i>num</i> – 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 <i>num</i> – 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: $MTU \text{ of the network} = MSS + \text{Size of TCP-IP Headers}$

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
<code>[no] custom message {session-created session-deleted} message_string</code>	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.
<code>[no] disable-log-by-destination</code>	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
<code>[no] enable-log-by-destination</code>	Enables logging by specific protocol, destination IP address, port, and range of ports. The following options are available: • <code>icmp</code> – enables logging for ICMP traffic • <code>ip</code> – configures a filter for IP entry • <code>ip6</code> – configures a filter for IPv6 entry • <code>others</code> – enables logging for other protocols • <code>tcp</code> – enables logging by destination TCP port • <code>udp</code> – enables logging by destination UDP port
<code>[no] facility options</code>	For the FW logging facility, specify one of the following <i>options</i>: • <code>kernel</code> (0: Kernel) • <code>user</code> (1: User-level) • <code>mail</code> (2: Mail) • <code>daemon</code> (3: System daemons) • <code>security-authorization</code> (4: Sec/authorization) • <code>syslog</code> (5: Syslog internal) • <code>line-printer</code> (6: Line printer) • <code>news</code> (7: Network news) • <code>uucp</code> (8: UUCP subsystem) • <code>cron</code> (9: Time-related) • <code>security-authorization-private</code> (10: Private security/authorization) • <code>ftp</code> (11: FTP) • <code>ntp</code> (12: NTP) • <code>audit</code> (13: Audit)

Parameter	Description
	• <code>alert</code> (14: Alert) • <code>clock</code> (15: Clock-related) • <code>local0</code> (16: Local use 0) (default) • <code>local1</code> (17: Local use 1) • <code>local2</code> (18: Local use 2) • <code>local3</code> (19: Local use 3) • <code>local4</code> (20: Local use 4) • <code>local5</code> (21: Local use 5) • <code>local6</code> (22: Local use 6) • <code>local7</code> (23: Local use 7)
<code>[no] format</code> <code>{ascii cef </code> <code>custom}</code>	Specify the firewall logging format: • <code>ascii</code> – A10 Text logging format (ASCII), used to support advanced CGN logging options, such as <code>include-radius</code> and <code>include-http</code>. • <code>cef</code> – Common Event Format for logging (default) • <code>custom</code> – Custom format for logging. This parameter must be configured to enable custom logging. Configure the arbitrary log message using the custom message command.
<code>[no] include-dest-fqdn</code>	Include the destination's Fully Qualified Domain Name (FQDN) string in the logs.
<code>[no] include-http options</code>	Include one or more of the following HTTP fields in http-request logs: • <code>cookie</code> – Log HTTP Cookie Header • <code>file-extension</code> – 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
<code>[no] include-radius-attribute options</code>	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
<code>[no] include-year</code>	Include the 4-digit year in the logs.
<code>[no] log http-requests {host</code>	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 <i>options</i>	The additional rules for FW logging events. Specify one of the following <i>options</i>: • 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 <i>group-name</i>	This option binds a service group to the logging template. <i>group-name</i> is the name of the service group. (1-127 characters)
[no] severity <i>options</i>	The minimum severity level for which log messages will be sent. Specify one of the following <i>options</i>: • 0 (emergency) • 1 (alert)

Parameter	Description
	• 2 (critical) • 3 (error) • 4 (warning) • 5 (notification) • 6 (information) • 7 (debugging) (default)
<code>[no] source-address {ipv4-add ipv6 ipv6-add}</code>	Specify the source address of logging packet.
<code>[no] session-periodic-log interval number</code>	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
<code>\$proto-name\$</code>	Protocol used in the session.	UDP/TCP

Keyword	Description	Example Output in logs
<code>\$src-ip\$</code>	Source IP address of the session.	5.5.5.100
<code>\$src-port\$</code>	Source Port number of the session.	34273
<code>\$dst-ip\$</code>	Destination IP address of the session.	6.6.6.100
<code>\$dst-port\$</code>	Destination Port number of the session.	2123
<code>\$in-interface\$</code>	Incoming network interface of the session.	ve801
<code>\$out-interface\$</code>	Outgoing network interface of the session.	ve701
<code>\$rule-set-name\$</code>	Specific rule set applied to the session.	rule-set1
<code>\$rule-name\$</code>	Specific rule name within the rule set that matched the session.	rule1
<code>\$partition-name\$</code>	Partition within the Firewall where the session exists.	p1
<code>\$sesn-start-time\$</code>	Start time of the session.	20190520062105
<code>\$sesn-start-time-epoch\$</code>	Epoch start time of the session.	1726081258
<code>\$time-stamp\$</code>	Log generation time stamp	20200510062005
<code>\$src-zone\$</code>	Source Zone	outside
<code>\$dest-zone\$</code>	Destination Zone	inside
<code>\$app-id\$</code>	App Id	5
<code>\$radius-msisdn\$</code>	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 Output in logs
face\$	session.	
\$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
\$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 Output 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-ctml,$radius-ctm2$
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-ctml$
```

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
<code>[no] fw vrid vrid-group</code>	Allow this ACOS device to join a VRRP-A group id. <i>vrid-group</i> The <i>vrid-group</i> 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
<i>category</i>	Specify application category
<i>clear</i>	Clear or reset functions
<i>do</i>	Run executorial commands in configuration mode
<i>end</i>	Exit from the configuration mode
<i>exit</i>	Exit from the configuration mode or the sub mode
<i>no</i>	Negate a command or set its defaults
<i>protocol</i>	Specify one or more applications
<i>show</i>	Display running system configuration
<i>user-tag</i>	Display customized tag
<i>write</i>	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 <i>name</i>	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
<i>notes</i>	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
<i>name</i>	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
<pre>[no] action {permit deny reset}</pre>	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.
<pre>[no] application { any category object-group protocol }</pre>	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
<pre>[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 </pre>	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 – <i>ip-addr</i> can be an ipv4-address Or any. • object – specify the name of the network object.

Commands under rule-set rule	Description and Sub-commands
<pre> virtual-server <i>srv-name</i> zone [any <i>zone-name</i>] } </pre>	• 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: In release 4.1.1 and later, 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.
<pre> [no] dscp {<i>dscp-value</i> range <i>dscp-start dscp-end</i>} </pre>	Configure the DSCP (Differentiated Services Code Point) match conditions, which can be one of the following: <i>dscp-value</i> - 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)

Commands under rule-set rule	Description and Sub-commands
	• 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) range - You can specify the range (0-63) by providing <i>dscp-start</i> and <i>dscp-end</i> values.
<pre>[no] idle- timeout num</pre>	Enter <i>num</i> for the TCP/UDP idle-timeout. This value can range from 1-2097151 seconds. In release 4.1.1 and later, ACOS offers the ability to configure idle-timeouts at the <i>rule</i> 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

Commands under rule-set rule	Description and Sub-commands
	individual rules within a rule-set. Port-based timeouts and rule-based idle-timeouts are only available for TCP and UDP, and can only be configured for destination ports.
<pre>[no] ip- version {v4 v6}</pre>	Set the IP version for this rule. • v4 – designates this as an IPv4 rule. • v4 – designates this as an IPv6 rule.
<pre>[no] move- rule { top before target-rule after target-rule bottom }</pre>	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<i>target-rule</i> – moves the rule before a designated rule in the rule-set. • after<i>target-rule</i> – moves the rule after a designated rule in the rule-set. • bottom – moves the rule to the bottom position in the rule-set.
<pre>[no] remark comment</pre>	Enter a comment or remark about this rule. Can be 1-255 characters.
<pre>[no] sampling- enable {all hit- count}</pre>	Enable baselining. Options are: • all – All • hit-count – Hit count

Commands under rule-set rule	Description and Sub-commands
<pre>[no] service { any icmp [code type] icmpv6 [code type] object-group name proto-id num tcp {dst src} udp {dst src} sctp [template name] }</pre>	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: ◦ eqport-num – Equal to the port number (1-65535). ◦ gtport-num – Greater than the port number (1-65535). ◦ ltport-num – Lower than the port number (1-65535). ◦ rangeport-num – The starting port number (1-65535). • udp – UDP. Specify dst or src and then specify the following sub-options: ◦ eqport-num – Equal to the port number (1-65535). ◦ gtport-num – Greater than the port number

Commands under rule-set rule	Description and Sub-commands
	(1-65535). ◦ ltp<i>port-num</i> – Lower than the port number (1-65535). ◦ range<i>port-num</i> – The starting port number (1-65535). • sctp – SCTP. Specify a SCTP template to be used.
<pre>[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]}</pre>	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 - <i>ip-addr</i> 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
<pre>[no] track- application</pre>	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
<code>listen-on-port</code>	Configure the permitted action as listen on the port.
<code>log</code>	Enable logging.
<code>cgnv6 [log lsn-lid fixed-nat static-nat ds-lite [lsn-lid inspect-payload]]</code>	Apply CGNv6 policy to the rule. Available options are: • <code>log</code> – Enable logging. • <code>lsn-lid</code> – 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
<code>cgnv6 [lsn-lid fixed-nat]</code>	Apply CGNv6 policy to the rule. Available options are: <code>lsn-lid</code> – Apply specified

Parameter	Description
	CGNV6 LSN LID. fixed-nat – Apply CGNV6 Fixed NAT. Note: • 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

Parameter	Description
	action Forward.
ipsec <i><VPN IPsec name></i>	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 <i><template_num></i>	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

Parameter	Description
	Control rule-set.
<code>listen-on-port</code>	Configure the permitted action as listen on the port.
<code>log</code>	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. • <code>fw-logging-template <fw template name></code> • <code>cgnv6-logging-template <CGNv6 template name></code> • <code>netflow-monitor <monitor</code>

Parameter	Description
	name>
respond-to-user-mac	Assigns the route hop based on the MAC address inside the client's request on the packets matching the rule. This option is disabled by default.
set-dscp <i><dscp-value></i>	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)

Parameter	Description
	• 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

Parameter	Description
	<pre>(precedence 1) dscp (001000)</pre> • 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) • <1-63> - The DSCP value. Enter a value

Parameter	Description
	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-open on-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

Parameter	Description
	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 <code>fw tcp syn-cookie</code> command. The following scenarios describe the behavior: • if <code>permit tcp syn-cookie</code> is disabled for a firewall rule, and the global <code>fw tcp syn-cookie</code> command is enabled with

Parameter	Description
	a specific threshold and timeout, ACOS does not consider the global configuration and disables syn-cookie protection for the traffic matching the rule. • if <code>permit tcp syn-cookie</code> is enabled for a firewall rule, and the global <code>fw tcp syn-cookie</code> command is also enabled with a specific threshold and timeout, ACOS does not consider the threshold and timeout for the traffic matching the

Parameter	Description
	rule. For this traffic, syn-cookie protection is always enabled.

Parameter	Description
	N- O- T- E: This command can not be configured when the firewall is down or not started.

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 <i>template_num</i>	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. You can specify a value between 1 to 1023. NOTE: Only supported for Packets-Per-Second downlink traffic.

Parameter	Description
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 <i>template_num</i>	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 Reset action allows the TCP sessions, that are being reset, to be tracked separately. You can specify a value between 1 to 1023.

Parameter	Description
	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
<i>any</i>	Any application.
<i>category</i>	Specify application category.
<i>object-group</i>	Specify object group of the application.
<i>protocol</i>	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.
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
<code>class-list</code>	Match destination IP against class-list.
<code>geo list</code>	Geo-location list for filtering.
<code>domain list</code>	Domain name list for filtering at destination firewall.
<code>ipv4-address</code>	IPv4 address of the selected option.
<code>ipv6-address</code>	IPv6 address of the selected option.
<code>object</code>	Pre-defined network object.
<code>object-group</code>	Pre-defined network object group.
<code>server</code>	SLB Real server name.
<code>threat-list</code>	Bind threat-list for source IP based filtering.
<code>zone</code>	Configure destination zone.
<code>name</code>	Name of the selected option like geo-location list,

Parameter	Description
	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
<code>[no] accounting</code>	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.

Command	Description
	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. • ignore – Ignore the entry. • delete-entry – Delete the entry.
[no] attribute <i>attr-name</i> [[vendor <i>vendor-id</i>] number <i>attr-id</i>]	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.

Command	Description
	• 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 MSISDN, or IMEI, and so on. For example, if your RADIUS server normally sends the MSISDN attribute as attribute 31, you could use the following command to configure the ACOS device to use the same attribute value for MSISDN: <pre>attribute msisdn number 31</pre>
<pre>[no] derived-attribute [usergroup userid] attribute { imei imsi msisdn custom1-6 regex reg-</pre>	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

Command	Description
<code>ular-expression }</code>	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 <i>regex</i> – 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 <code>([^\@]+)</code> and the data as 'username@domain', ACOS extracts and stores the first sub-string 'username'. ◦ With the pattern <code>@(\w+)</code> and the data 'username@domain', ACOS extracts and stores the first sub-string 'domain'. The regular expression supports the hexadecimal string. For example, <code>([^\x40]+)</code> will be interpreted in the backend as <code>([^\@]+)</code>, where <code>\x40</code> represents the <code>@</code> character in hexadecimal.

Command	Description
	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 <i>portnum</i>	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 <i>shared-secret</i>	Specifies the password string the external RADIUS servers and ACOS device use to authenticate RADIUS traffic between them.
[no] vrid <i>num</i>	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.
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.

Parameter	Description
<code>tunnel-timeout</code> <code>{seconds}</code>	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 <i>num</i>	Set the International Mobile Subscriber Identity (IMSI) number as a filter to block traffic from a country or a region.
selection-mode { mobilestation network verified } [imsi <i>num</i>]	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

Parameter	Description
	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 if 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 if 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 if 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-msisdn-list configuration mode for to modifying the NAME-070 msisdn-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 if 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
<code>[no] limit-concurrent-sessions num log</code>	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.
<code>[no] limit-cps num [burstsize bucket_size relaxed]</code>	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.
<code>[no] limit scope</code>	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. • subscriber-ip - The rate limiting policy is applied at a subscriber IP level defined in the rule.

Parameter	Description
	• subscriber-prefix <i>prefix_len</i> - 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 <i>num</i>	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. Specifying this option, places the template limit-policy in a rate-limit hierarchy. This causes the rate-limit entries based on this template limit-

Parameter	Description
	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 <code>parent</code> by any other template limit-policy) can be bound to the Traffic Control rules.
<code>max-min-fair</code>	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.
<code>relaxed</code>	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 <code>limit-cps</code> or <code>limit-throughput</code> command.
<code>user-tag</code>	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] <i>pps</i>	Configure the PPS rate limit. The following options are available: • downlink - Downlink traffic • uplink - Uplink Traffic • total - Sum total of downlink and uplink traffic <i>pps</i> - Specify the PPS threshold limit (1 to

Parameter	Description
	2147483647).
burstsize <i>bucket_size</i>	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 <i>num</i>	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 (<i>num</i>). 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
<code>[downlink total uplink] throughput [Mbps Kbps Gbps]</code>	Configure the throughput rate limit. The following options are available: <code>downlink</code> - Downlink traffic <code>uplink</code> - Uplink Traffic <code>total</code> - Sum total of downlink and uplink traffic <code>throughput</code> - 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 <i>bucket_size</i> [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
<code>checksum-check {enable}</code>	Enable checksum check on SCTP packets.
<code>half-open-idle-timeout {seconds}</code>	Set SCTP half-open timeout in seconds.
<code>idle-timeout {minutes}</code>	Set SCTP idle timeout in minutes.
<code>log {payload-proto-filtering}</code>	Log Payload Protocol IDs Filtered.
<code>permit-payload-protocol {iua m2ua m3ua sua m2pa h.323}</code>	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 <i>name</i>	Create a new Traffic Control rule-set. Use <code>traffic-control active-rule-set</code> 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
<i>notes</i>	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
<i>name</i>	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. • 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 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
<pre>[no] action-group [no] action { limit-policy num}</pre>	Configure the action in the action group by specifying the rate limit policy.
<pre>[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]}</pre>	Configure the destination match conditions, which can be one of the following: • class list <i><name></i> - Pre-configured class-list name. • domain-list <i><name></i> - Pre-configured domain-list name. • geolocation list <i><name></i> - 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 - <i>ip-addr</i> can be an ipv4-address or <i>any</i>. • 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.
<pre>[no] ip-version {v4 v6 any}</pre>	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.
<code>[no] remark comment</code>	Enter a comment or remark about this rule. It can be 1-255 characters.
<code>[no] sampling-enable {all hit-count}</code>	Enable baselining. Options are: • all – All • hit-count – Hit count
<code>[no] service {</code> <code>any </code> <code>icmp [code type] </code> <code>icmpv6 [code type] </code> <code>object-group name </code> <code>proto-id num </code> <code>tcp {dst src} </code> <code>udp {dst src} </code> <code>sctp [template name]</code> <code> }</code>	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<i>port-num</i> – Equal to the port number (1-65535). ◦ gt<i>port-num</i> – Greater than the port number (1-65535). ◦ lt<i>port-num</i> – Lower than the port number (1-65535). ◦ range<i>port-num</i> – The starting port number (1-65535). • udp – UDP. Specify dst or src and then specify the following sub-options: ◦ eq<i>port-num</i> – Equal to the port number (1-65535). ◦ gt<i>port-num</i> – Greater than the port number (1-65535). ◦ lt<i>port-num</i> – Lower than the port number (1-65535). ◦ range<i>port-num</i> – The starting port number (1-65535). • sctp – SCTP. Specify a SCTP template to be used.
<pre>[no] source [class-list name [type radius derived-attribute {usergroup userid}] geolocation [list entry] black- list]{ ipv4-address [ip-addr any] </pre>	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
<pre> object <i>obj-name</i> object-group <i>grp-name</i> server <i>srv-name</i> zone [any <i>zone-name</i>]} </pre>	• 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 - <i>ip-addr</i> 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
<code>[no] zone <i>name</i></code>	Create a new zone.
<code>[no] interface <i>option</i></code>	The the following interface options are available: <code>ethernet <i>port-num</i></code> – 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. • <code>lif logicalinterface-id</code> – 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. • <code>trunk num</code> – 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. • <code>tunnel num</code> – The configured interface is a tunnel. The tunnel interface ID takes a range of values from 1 to 128. • <code>ve ve-num</code> – 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.
<code>[no] local-type</code>	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 <code>any</code>. 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 <code>local-type</code> 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.
<code>[no] vlan vlan-id to vlan-id</code>	Configure a virtual LAN (VLAN) by replacing <i>vlan-id</i> with the ID of the VLAN (2-4094), followed by the <code>to</code> command. Then specify the <i>vlan-id</i> 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
<code>esp</code>	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 mismatch in Call IDs on PPTP call requests.
Call ID Mismatch on Call Reply	The number of instances where there is a mismatch 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
```

Firewall

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 Aggregate

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
1141a                      1141a.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
web-search-engines
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 <i>ipv-addr</i> ipv6-address <i>ipv6-addr</i>]
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 <i>ipv4-prefix</i>	View limit entries for the specified IPv4 prefix.
prefix6 <i>ipv6-prefix</i>	View limit entries for the specified IPv6 prefix.
rule-name <i>rule-name</i>	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 <i>custom_string</i>	Logging keywords for session creation events.
session-deleted <i>custom_string</i>	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
<i>string-value NAME</i>	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.
<i>ipv4_address</i>	Display the rate limit information for the specified IPv4 address.
<i>ipv6_address/nn</i>	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).
<i>modifier</i>	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
<code>clause-per-obj-grp</code>	Display the number of clauses per object group.
<code>helper-sessions</code>	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.
<code>ip-range</code>	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.
<code>object</code>	Display the resource usage information for firewall objects.
<code>object-group</code>	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
<code>internal</code>	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
```

NOTE: For Thunder 14045 devices, the output is displayed only for Master. For Thunder 7650 devices, the output is displayed only for one instance of the processing unit.

Example The following example shows sample output for the `show fw status` command on a multi-PU platform:

```
Master:

Current Active Rule-set           : rule7
Previous Successful Compilation Attempt : 2017-07-19
09:56:47
Previous Successful Compilation Duration : Less than a
millisecond
Most Recent Compilation Attempt    : 2017-07-19
09:56:47
Most Recent Compilation Status     : Successful

Blade 1:

Current Active Rule-set           : rule7
Previous Successful Compilation Attempt : 2017-07-19
09:56:47
Previous Successful Compilation Duration : Less than a
millisecond
Most Recent Compilation Attempt    : 2017-07-19
09:56:47
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.

Field	Description
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 Compilation Status	Status of most recent rule-set compilation: • 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 chassis 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.

Parameter	Description
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
<i>name 1-127</i>	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]
  [to zone-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 <i>name</i> .
from <i>zone-name</i>	Name of the zone from which traffic is coming.
to <i>zone-name</i>	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 chassis platform, 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
                critico                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
Traffic 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

```


Firewall

```

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

```

Firewall

```

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.

Field	Description
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.
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
37048xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2w
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 <i>value</i>	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 ID. The length of the <code>derived-attribute-value</code> can be 1-63.
imei <i>string</i>	Shows information associated with the IMEI.
imsi <i>string</i>	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.
<i>attr-name</i>	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 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 database update.
Connection Status	Indicates the status of the connection.

Field	Description
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 <i>num</i>	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 <i>name</i>	View statistics for the Traffic Control rule-set. Specify the rule-set name (1-63 characters).
rule-name <i>name</i>	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
<code>statistics</code>	Clear DDoS statistics.
<code>dest</code>	Clear DDoS destination entry information.
<code>[ip-entries ip-incidents] [address ipv4-address all]</code>	Clear DDoS destination information for the IP entries or the IP incidents. You can clear the entries or incidents for one of the following: • <code>address ipv4-address</code> - Clear DDoS destination entry information for the specified IPv4 address. • <code>all</code> - 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.
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
<code>ipv4</code>	This is an optional parameter that allows you to clear only the IPv4 SMP helper sessions.
<code>ipv6</code>	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 {usergroup 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 <i>string</i>	Clears information associated with the IMEI.
imsi <i>string</i>	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 <i>resp_code</i>	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 <i>msg</i> custom- page <i>page</i>	Display a custom message when a request is blocked by NGWAF. The message can be displayed by specifying one of the following: • <i>msg</i> - A block message with a maximum length of 1023 characters. • custom-page <i>page</i> - 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
	• <code>\$a10_ngwaf_session_id\$</code> - The session ID. • <code>\$a10_ngwaf_uri\$</code> - The request URI. NOTE: The keywords are case-sensitive and only 4 keywords can be used in a message or custom webpage.
<code>custom-signal-clist</code> <i>string_list</i>	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.
<code>monitor-mode-enable</code>	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 <code>marked</code> 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.
<code>pre-process-enable</code> <i>exp_time</i>	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
	<i>exp_time</i> - 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.
<pre>use-https- proxy { ipv4_address ipv6_ address } portnum</pre>	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: <i>ipv4_address</i> - Proxy server IPv4 address OR <i>ipv6_address</i> - Proxy server IPv6 address <i>portnum</i> - 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.
<pre>use-mgmt- port</pre>	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
<code>access_key</code>	Enter the NG-WAF agent access-key ID (1-64 characters).
<code>secret_key</code>	Enter the NG-WAF agent secret access key ID (1-64 characters).

Mode Configuration mode

NOTE: This command is not synchronized in a Virtual Chassis System (VCS). 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  
aaaaaAAAAA11111222222CCCccttr
```

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.
<i>virtual_port_name</i>	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 .
<i>virtual_server_name portnum</i>	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:    2xxxxxxxxx
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:    2xxxxxxxxx
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 14](#) describes all the possible fields in the command output.

Table 14 : 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 14 : 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
<i>virtual_server_name</i>	Specify the name of the virtual server (1-128 characters).
<i>portnum</i>	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 15 : 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 15 : 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 of 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 15 : 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 15 : 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 15 : 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 15 : 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 Create 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
<code>name</code>	Specify the name of the certificate. ACOS (config)# pki acme-cert test
<code>account-email</code>	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@examplomain.com
<code>acme-client</code>	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. <pre>ACOS (config-acme cert:test)# acme- client agent-v1</pre>
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. <pre>ACOS (config- acme cert:test)# cert- type rsa rsa-key-length 2084</pre> - 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. <pre>ACOS (config- acme cert:test)# cert- type ecdsa ec-key-length 384</pre>
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. <pre>ACOS (config- acme cert:test)# domain exampledomain.com</pre>
eab-hmac-key {name encrypt-}	Specify the HMAC key for ACME External Account Binding (EAB).

Parameter	Description
ted <i>name</i> }	The MAC key should be in base64url-encoded format. <i>name</i> - Specify the HMAC key. encrypted <i>name</i> - Specify the A10 reserved encrypted password. Do not use this option manually. <pre>ACOS (config- acme cert:test)# eab-hmac-key _bn_xA1sxtf7Nd1-1JWHLa24GCy8mwDEfYvehJmxRVWFdJ-41BOQNdN9Q-JtTQYKZyUDjNfU7Aen_6DJ22gYA</pre>
eab-key-id <i>name</i>	Specify the key identifier for ACME EAB. The key identifier must be an ASCII string. <pre>ACOS (config- acme cert:test)# eab-key-id OBUBsbGsqLa5_Iw9EnbC7g</pre>
enroll	Initiate the device enrollment (staging or force) with the CA certificate. <pre>ACOS (config- acme cert:test)# enroll</pre>
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	Ignore the next renewal time and forced to renew.
log-level {1 2}	Specify the logging level output of the ACME commands. The following options can be configured:

Parameter	Description
	• 1 - Enable the default and basic logging level. • 2 - Enable the detailed logging level, which includes debugging messages. <pre>ACOS (config- acme cert:test)# log-level 2</pre>
verification-waiting-time	Specify how long (in seconds) the ACME client should wait for the CA certificate to verify the challenge token.
renew-before <i>{hour day week month}</i>	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) <pre>ACOS (config- acme cert:test)# renew-before month 1</pre>
renew-every <i>{minute hour day week month}</i>	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 <i>hour 8</i>
san-domain <i>{dns}</i>	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 <i>test.com</i>
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 <i>https://www.caserver.com/testing</i>
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 <i>https://www.caserver.com/staging</i>
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 <i>1</i>

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_xAlsxtf7Nd1-
1JWHLa24GCy8mwDEfYvehJmxRVWFdJ-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
<code>agent-v1</code>	Sets <code>agent-v1</code> as the ACME client for the ACME enrolment or renewal. This is the default value.
<code>agent-v2</code>	Sets <code>agent-v2</code> 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
<i>level</i>	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
<i>hour</i>	Number of hours before the certificate expiry. The value of renewal period is between 1-255.
<i>day</i>	Number of days before the certificate expiry. The

Parameter	Description
	value of renewal period is between 1-255.
<i>week</i>	Number of weeks before the certificate expiry. The value of renewal period is between 1-255.
<i>month</i>	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
<i>minute</i>	Periodic interval in minutes. It is between 2-255.
<i>hour</i>	Periodic interval in hours. It is between 1-255.
<i>day</i>	Periodic interval in days. It is between 1-255.
<i>week</i>	Periodic interval in weeks. It is between 1-255.
<i>month</i>	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
<i>num</i>	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 concurrent process	Maximum # of concurrent 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
<i>source-cert-name</i>	Name of the existing SSL certificate file (1-63 characters).
rotation	Specify the rotation number of the SCEP generated certificate file (1-4).
<i>dest-cert-name</i>	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 <i>dest-cert-name</i> , 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
<i>source-cert-name</i>	Name of the existing SSL key file (1-63 characters).
rotation	Specify the rotation number of the SCEP generated key file (1-4).
<i>dest-cert-name</i>	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 <i>dest-key-name</i> , 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
<i>rsa</i>	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.
<i>ecdsa</i>	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
<i>name</i>	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
<i>name</i>	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
<i>level</i>	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
<i>seconds</i>	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
<i>OID</i>	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
<i>hour</i>	Number of hours before the certificate expiry. The value of renewal period is between 1-255.
<i>day</i>	Number of days before the certificate expiry. The value of renewal period is between 1-255.
<i>week</i>	Number of weeks before the certificate expiry. The value of renewal period is between 1-255.
<i>month</i>	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
<i>minute</i>	Periodic interval in minutes. It is between 2-255.
<i>hour</i>	Periodic interval in hours. It is between 1-255.
<i>day</i>	Periodic interval in days. It is between 1-255.
<i>week</i>	Periodic interval in weeks. It is between 1-255.
<i>month</i>	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
<i>name</i>	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
<i>certtype</i>	Specify the encryption algorithm to be used.

Parameter	Description
	- rsa - RSA certificate - ecdsa - ECDSA certificate
<i>csr csr-name</i>	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 certificate.
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
<i>cert-name</i>	Deletes a specific self-signed certificate.
days <i>num</i>	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
<i>name</i>	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
<i>seconds</i>	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
<i>bit key</i>	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
<i>level</i>	<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
<i>seconds</i>	<15-432000>.

Default 180 seconds

Mode SCEP certificate mode

method

Description HTTP request method used for enrollment.

Syntax `[no] method {GET | POST}`

Parameter	Description
<i>seconds</i>	<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
<code>password</code>	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
<code>day</code>	Units of time, 1-255.
<code>hour</code>	Units of time, 1-255.
<code>month</code>	Units of time, 1-255.
<code>week</code>	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
<code>minute</code>	Periodic interval in minutes, 2-255.

Parameter	Description
<i>hour</i>	Periodic interval in hours, 1-255.
<i>day</i>	Periodic interval in days, 1-255.
<i>week</i>	Periodic interval in weeks, 1-255.
<i>month</i>	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
<i>dns</i>	Units of time, 1-255.
<i>email</i>	Units of time, 1-255.
<i>ip</i>	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
<i>num</i>	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
<i>num</i>	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 FPGA 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>
<i>gateway-name</i>	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 <i>string</i>	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 <i>hash</i>	Uses RSA certificate-based authentication to authenticate the remote gateway. <i>hash</i> - 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 <i>hash</i>	Uses an ECDSA certificate-based authentication to authenticate the remote gateway. <i>hash</i> - 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
<i>group-num</i>	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
<i>seconds</i>	Specify the number of seconds between DPD R-U-THERE messages. The range can be 1-3600 seconds.
<i>num</i>	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
<i>encrypt-alg</i>	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: <u>aes-gcm-128, aes-gcm-192, and aes-gcm-256 are supported in IKEv2 Gateway only.</u> • null - No encryption.
<i>hash-alg</i>	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: <u>For <i>hash-alg</i> the value cannot be null. So, this is an unsupported, discontinued, and older value.</u>
priority <i>num</i>	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
<i>passphrase</i>	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
<i>seconds</i>	IKE SA age in seconds. You can specify 300-86400 <i>seconds</i> .

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
<i>ip</i>	Valid IPv4 address.
<i>ipv6</i>	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
<i>filename</i>	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
<i>string</i>	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
<i>domain-name</i>	Remote IP based on the domain name.
<i>ipaddr</i>	Valid IPv4 address.
<i>ipv6addr</i>	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
<i>filename</i>	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
<i>string</i>	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 <code>vrvid</code> command, the <code>default</code> option is not applicable and available now.
<i>num</i>	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 <i>name</i>	Primary RADIUS authentication server. It is of 1-63 characters.
sec <i>name</i>	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
<i>seconds</i>	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
<i>tunnel-name</i>	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
<i>bits</i>	You can 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
<i>num</i>	
<i>ipaddr</i>	

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 <i>filename</i>	Primary CRL File Name or URL (http://www.example.com/ocsp) (only .der filetypes).
sec <i>filename</i>	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
<i>group-num</i>	• 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
<i>pri ip address</i>	Primary DHCP Server IP Address.
<i>sec ip address</i>	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
<i>encrypt-alg</i>	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.
<i>hash-alg</i>	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 Message-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 Ignores the next renewal time and forces to renew certificate.

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
<i>fragment-size</i>	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
<i>gateway-name</i>	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
<i>Mb</i>	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
<i>seconds</i>	The IPsec SA age in seconds. You can specify 300-28800 <i>seconds</i> .

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
<i>bytes</i>	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 <i>ipaddr</i>	Specify the local traffic selector IPv4 address.
local <i>netmask</i>	Specify the IPv4 address network mask.
local <i>port</i>	Specify the port number.
local <i>protocol</i>	Specify the IP Protocol Number, 0-255.
remote <i>ipaddr</i>	Specify the IP address of the interface that terminates the tunnel.
remote <i>netmask</i>	Specify the IPv4 Address Network Mask.
remote <i>port</i>	Specify the UDP port number.
remote <i>protocol</i>	Specify the IP protocol number, 0-255.
<i>ipv6addr</i>	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
<i>group-name</i>	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 <i>ipsec-name</i>	Specify one of the tunnels as a group member.
priority <i>pri-value</i>	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
<i>revocation-name</i>	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
<i>filename</i>	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 <i>server</i>	Primary OCSP authentication server, 1-31 characters.
sec <i>server</i>	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	<code>[no] vpn tcp-mss-adjust-disable</code>
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} log name`

Parameter	Description
<code>acme-cert</code>	Clears the ACME certificate related information.
<code>scep-cert</code>	Clears the SCEP certificate related information.
<code>log <i>name</i></code>	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
<i>gateway-name</i>	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
<i>gateway-name</i>	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
<i>group-name</i>	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
<i>tunnel-name</i>	Specify the IPsec tunnel name.
<i>all-partitions</i>	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 ocsip

Description Clear OCSIP information.

Syntax `clear vpn ocsip`

Default	N/A
Mode	Global configuration mode

debug monitor

Description	Show all currently active debug output on terminal.
Syntax	<code>debug monitor</code>
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	<code>debug packet {count detail interface l3-protocol l4-protocol}</code>

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 Error	0	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 Packets	0	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 FPGA, 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
<i>gateway-name</i>	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
                sha256
Lifetime:      358s
method:        preshare-key
DH group:      2
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
                sha256

```

Hash:

Auth-

NAT-

Hash:

```

Lifetime:      202s
method:    preshare-key
DH group:      2
T:            disabled
Status:        Established
Auth-
NAT-

```

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
<code>all-partitions</code>	VPN configuration summary of all partitions.
<code>gateway-name</code>	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
Initiate Rekey:0
Child SA Rekey:0
Outgoing Init Request:1
Outgoing Init Response:0
Outgoing Auth Request:0
Request:0
Outgoing Auth Response:0
Response:0
Outgoing Create Child Request:0
Outgoing Create Child Response:0
Outgoing Info Request:0
Outgoing Info Response:1
Respond Rekey:0
Incoming Init Request:0
Incoming Init Response:1
Incoming Auth Request:0
Incoming Auth Response:0
Incoming Create Child
Incoming Create Child
Incoming Info Request:1
Incoming Info Response:0
Incoming Invalid SPI:0

```

```

Incoming Invalid:0
Gateway: 39
Initiate Rekey:0
Respond Rekey:0
Incoming Init Request:0

Child SA Rekey:0
Outgoing Init Request:0
Outgoing Init Response:0
Outgoing Auth Request:0
Request:0
Outgoing Auth Response:0
Response:0
Outgoing Create Child Request:0
Outgoing Create Child Response:0
Outgoing Info Request:0
Outgoing Info Response:0
Incoming Invalid:0
Gateway: 40
Initiate Rekey:0
Child SA Rekey:0
Incoming Init Response:0
Incoming Auth Request:0
Incoming Auth Response:0
Incoming Create Child
Incoming Create Child
Incoming Info Request:0
Incoming Info Response:0
Incoming Invalid SPI: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
<code>partition</code>	VPN configuration summary per partition.
<code>all-partitions</code>	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
<i>group-name</i>	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
<i>sa-name</i>	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
<code>follow</code>	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.
<code>from-start</code>	Lists the VPN log messages, starting with the first message in the buffer.
<code>num-lines</code> <code>num</code>	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 ocsf
  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 <i>port-num</i>	The configured interface is a virtual or physical Ethernet port with <i>port-num</i> ID. The port ID takes a range of values that depends of the platform ACOS is running on.
lif <i>logical-interface-id</i>	The configured interface is a logical interface in a Software Defined Network (SDN) or Overlay Network with <i>interface-id</i> ID. The logical interface ID takes a range of values from 1 to 128.

Parameter	Description
loopback <i>num</i>	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 <i>System Configuration and Administration Guide</i> .)
management2	The configured interface is the second management interface of the ACOS Device. (For more information, see <i>System Configuration and Administration Guide</i> .) NOTE: The second management interface is available only for the Thunder 8665S platform.
trunk <i>num</i>	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 <i>num</i>	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 <i>Configuring IPsec VPN</i> .)
ve <i>ve-num</i>	The configured interface is a virtual Ethernet Interface. (For more information, see “Virtual LAN Support” in the <i>Network Configuration Guide</i> .) 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
<i>num</i>	Number or ID of a configured ACL.
<i>name</i>	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 <i>key-id</i> { 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 <i>ms</i> min-rx <i>ms</i> multiplier <i>num</i>	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 <i>ms</i> 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 <code>[ipv4 {local-address neighbor-address}]</code> <code>ipv6 {local-address neighbor-address}]</code>	Configures a Micro BFD. • ipv4 - IPv4 BFD sessions. ◦ <code>local-address</code> - Specify the IPv4 local address. ◦ <code>neighbor-address</code> - Specify the IPv4 neighbor address. • ipv6 - IPv6 BFD sessions. ◦ <code>local-address</code> - Specify the IPv6 local address. ◦ <code>neighbor-address</code> - 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	<code>[no] dac-link-training-enable</code>
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: <pre>ACOS(config-if:ethernet:12)#dac-link-training-enable</pre>

disable

Description	Disable an interface.
Syntax	<code>disable</code>
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: <pre>ACOS(config)# interface ethernet 3 ACOS(config-if:ethernet:3)# disable</pre>

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
<i>normal-rate</i>	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
<i>max-rate</i>	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.
<i>lockup-time</i>	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
<i>normal-rate</i>	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 <i>max-rate</i>	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.
<i>lockup-time</i>	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	<code>[no] ip allow-promiscuous-vip</code>
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 <i>Application Delivery and Server Load Balancing Guide</i> .

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	<code>[no] ip cache-spoofing-port</code>
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 <i>Application Delivery Controller Guide</i> .
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	<code>[no] ip client</code>
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 Enable 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 live to reflect. As a result, if the SSH connection is restarted, the VCS floating IP to 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 is 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 will use the management route table for reply traffic on 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-response-time response-timer`

Parameter	Description
<i>query-timer</i>	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.
<i>response-timer</i>	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 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 runs 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
<i>ipaddr</i>	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 <i>key-string</i>	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 <i>number</i>	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 <i>seconds</i>	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 <i>seconds</i>	Number of seconds between transmission of OSPF Hello packets on this interface, 1-65535 seconds. The default is 10 seconds.
message-digest-key <i>key-id md5</i> <i>key-string</i>	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 <i>type</i>	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 <i>number</i>	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 <i>seconds</i>	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 <i>seconds</i>	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 <i>name</i> [<i>name</i> ...]	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 <i>auth-string</i> [<i>auth-string</i> ...]	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	<pre>[no] ip rip receive version {1 [2] 2}</pre> 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	<pre>[no] ip rip receive-packet</pre>
Default	Enabled
Mode	Interface

ip rip send version

Description	Specify the RIP version allowed to be sent on the interface.
Syntax	<pre>[no] ip rip send version {1 [2] 2}</pre> 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	<code>[no] ip server</code>
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	<code>[no] ip slb-partition-redirect</code>
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
<code>inside</code>	Inside (private) interface for the stateful firewall.
<code>outside</code>	Outside (public) interface for the stateful firewall.
<code>access-list</code>	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 address ipaddr/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
<i>name</i>	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
<i>ipv6-addr</i>	Valid unicast IPv6 address.
<i>prefix-length</i>	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 <i>seconds</i>	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 <i>num</i>	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 <i>seconds</i>	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 <i>seconds</i>	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, see RFC 4861 .
prefix <i>ipv6- addr/prefix- length [options]</i>	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 <i>seconds</i> – Specifies the number of seconds for which auto-generated addresses remain preferred. You can specify 0-4294967295 seconds. The default is 604800. • valid-lifetime <i>seconds</i> – 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 <i>num</i>	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
<i>ms</i>	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 <i>seconds</i>	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 <i>num</i>	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
<i>ipv6-addr</i>	IPv6 address of the OSPF neighbor.
cost <i>num</i>	Specifies the link-state metric to the neighbor, 1-65535. There is no default cost set.
poll-interval <i>seconds</i>	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 <i>num</i>	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.
<i>num</i>	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
<code>inside</code>	Inside (private) interface for the stateful firewall.
<code>outside</code>	Outside (public) interface for the stateful firewall.
<code>access-list</code>	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 <i>name</i> [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	<code>[no] isis bfd disable</code>
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	<code>[no] isis circuit-type [level-1 level-1-2 level-2]</code> 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
<i>seconds</i>	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
<i>seconds</i>	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
<i>num</i>	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
<i>group-num</i>	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.
<i>blocked</i>	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
<i>num</i>	Specifies the cost of using this interface as a link in an IS-IS route. You can specify 1-63.
<i>level-1</i> <i>level-2</i>	Specifies the IS-IS routing level to which the default metric setting applies: • <i>level-1</i> – Intra-area • <i>level-2</i> – Inter-area The default is <i>level-1</i> .

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
<i>string</i>	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
<i>num</i>	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
<i>seconds</i>	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
<i>num</i>	Specifies the metric length. You can specify 1-16777214.
<i>level-1</i> <i>level-2</i>	Specifies the IS-IS routing level to which the metric applies: • <i>level-1</i> – Intra-area • <i>level-2</i> – Inter-area The default is <i>level-1</i> .

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 this interface.
Syntax	<code>[no] l3-vlan-fwd-disable</code>
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 leaf 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	<code>[no] lldp enable [rx] [tx]</code>

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
<code>vlan</code>	Assign a name to the VLAN and map the VLAN ID to the VLAN.
<code>link-aggregation</code>	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: <pre>ACOS(config) # mirror-port 1 ethernet 1 both</pre>
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: <pre>ACOS(config) # mirror-port 2 ethernet 2 input</pre>
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: <pre>ACOS(config) # mirror-port 3 ethernet 3 output</pre>
vlan <i>vlan-id</i>	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
<i>number-of-ports</i>	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 <i>seconds</i> [do-auto-recovery]	In the <code>do-auto-recovery</code> 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 <code>do-auto-recovery</code> 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-FPGA 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
<i>TrunkID</i>	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 | 13-vlan-fwd-disable]}
  {traffic-type}
  {traffic-source}
  {traffic-destination}
  {more-options}
}

```

Match Option	Description
<i>sequence-number</i>	Sequence number of this rule in the ACL. You can use this option to resequence the rules in the ACL.
remark <i>string</i>	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 13-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 specifies 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. 13-vlan-fwd-disable - Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
<i>traffic-type</i>	Specifies the type of traffic to match: geo-location - Matches on geo-location name. icmp [type {<i>type-option</i>} [code {any-code <i>code-num</i>}]] - Matches on ICMP traffic. ip - Matches on any type of IP traffic. object-group <i>group-name</i> - Matches on the values in the specified service object group. tcp - Matches on TCP traffic. udp - Matches on UDP traffic.
<i>traffic-source</i>	Specifies the source address(es) on which to match: any - The ACL matches on all source IP addresses. host <i>host-src-ipaddr</i> - The ACL matches only on the specified host IP address. net-src-ipaddr {<i>filter-mask</i> <i>/mask-length</i>} -

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 <i>filter-mask</i> filters on a 24-bit subnet: 0.0.0.255 Alternatively, you can use <i>mask-length</i> 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 <i>group-name</i> – Matches on the addresses in the specified network object group.
eq <i>src-port</i> gt <i>src-port</i> lt <i>src-port</i> range <i>start-src-port</i> <i>end-src-port</i>	These options are available for both TCP or UDP only; they specify the source protocol ports on which to match: • eq <i>src-port</i> – The ACL matches on traffic from the specified source port. • gt <i>src-port</i> – The ACL matches on traffic from any source port with a higher number than the specified port. • lt <i>src-port</i> – The ACL matches on traffic from any source port with a lower number than the specified port. • range <i>start-src-port end-src-port</i> – 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
<i>more-options</i>	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 <i>vlan-id</i> – Matches on the specified VLAN. VLAN matching occurs for incoming traffic only. • dscp<i>num</i> – 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 virtual chassis, use the `device-context` command to specify the device in the chassis 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
<i>bad-content</i>	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 oversized 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
<i>regular-expression</i>	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
<i>num</i>	List number.
{ expanded standard } <i>list-name</i>	List type and name.
deny permit	Action to perform for matching communities.
<i>community-number</i>	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 } <i>list-name</i>	List type and name.
<i>num</i>	List number.
deny permit	Action to perform for matching communities.
<i>community-number</i>	Community number in XX:YY:ZZ format.

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 chassis 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 <code>ip dmz</code> command can be configured under <code>interface ethernet</code> as well as <code>interface ve</code> .

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
<i>num</i>	List number.
{ expanded standard } <i>list-name</i>	List type and name.
deny permit	Action to perform for matching communities.
rt soo { <i>AS-num:nn</i> <i>ipaddr:nn</i> }	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
<i>max-use</i>	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.
<i>min-use</i>	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 virtual chassis, use the `device-context` command to specify the device in the chassis 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 virtual chassis, use the `device-context` command to specify the device in the chassis to which this command must apply.

ip icmp disable

Description Disables ICMP messages.

Syntax `[no] ip icmp disable {redirect | unreachable}`

Parameter	Description
<code>redirect</code>	Disables sending of ICMP Redirect messages.
<code>unreachable</code>	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
<code>always-source-nat-errors</code>	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.
<code>respond-to-ping</code>	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 <i>name</i>	Specifies a class list. Entries in the class list map internal IP addresses to IP NAT pools.
list <i>acl-name</i>	Specifies an ACL that matches on the inside addresses to be translated.
pool <i>pool-or-group-name</i> [msl <i>seconds</i>] [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 <i>inside-ipaddr</i>	Statically maps the specified inside address to a specific NAT address.

Parameter	Description
<i>nat-ipaddr</i>	
disable enable	Disables or re-enables the static mapping.
vrid <i>num</i>	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
<i>pool-name</i>	Name of the address pool.
<i>start-ipaddr</i>	Beginning (lowest) IP address in the range.
<i>end-ipaddr</i>	Ending (highest) IP address in the range.
netmask { <i>subnet-mask</i> <i>/mask-length</i> }	Network mask for the IP addresses in the pool.
gateway <i>ipaddr</i>	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 <code>port-overload</code> 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 <i>device-id</i>	Configure the Scale Out device ID to which this IP NAT pool will be bound (1-64).
vrid <i>num</i>	VRRP-A VRID. In the shared partition, you can specify 1-31 or <code>default</code> . In private partitions, you can specify <code>default</code> .

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
<i>pool-group-name</i>	Name of the pool group.
vrid <i>num</i>	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
<i>list-name</i>	Name of the static NAT address range.
<i>local-ipaddr /mask-length</i>	Beginning (lowest) IP address in the range of local addresses.
<i>global-ipaddr /mask-length</i>	Beginning (lowest) IP address in the range of global addresses.
count <i>number</i>	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 <i>acl-label</i>	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 <i>acl-name</i> — Specifies a named ACL.
vrid <i>num</i>	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
<code>[no]</code> facility <i>facility-name</i>	Specifies the logging facility to use. For a list of available facilities, enter the following command: facility ? The default facility is local0.
<code>[no]</code> include-destination	Includes the destination IP addresses and protocol ports in NAT port mapping logs.
<code>[no]</code> include-rip-rport	Includes the IP and port of real server in logs (SLB function only).
<code>[no]</code> 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 <i>group-name</i>	Specifies the service group for the external log servers.
[no] severity <i>severity-level</i>	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 { <i>source-port</i> 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 <i>seconds</i> 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 <i>seconds</i> 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 <code>tcp-timeout</code> or <code>udp-timeout</code> setting is used. For UDP port 53, the SLB MSL time is used.
<code>tcp-timeout</code> <i>seconds</i>	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.
<code>udp-timeout</code> <i>seconds</i>	The supported values and timer behavior for UDP sessions are the same as those for <code>tcp-timeout</code> (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
<i>list-name</i>	Name of the IP prefix list. The name cannot contain blanks.
description <i>string</i>	Description of the IP prefix list.
seq <i>sequence-num</i>	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 <i>ipaddr</i> <i>/mask-length</i>	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 <i>prefix-length</i>	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 <i>prefix-length</i>	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
<i>protocol</i>	• <code>connected</code> - Physically connected • <code>ebgp</code> - External Border Gateway Protocol • <code>ibgp</code> - Internal Border Gateway Protocol • <code>isis</code> - Intermediate System to Intermediate System protocol • <code>ospf</code> - Open Shortest Path First protocol

Parameter	Description
	<code>rip</code> - Routing Information Protocol <code>static</code> - 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
<i>destination-ipaddr</i>	Specifies the destination of the route. To configure a default route, specify 0.0.0.0/0.

Parameter	Description
<i>{subnet-mask /mask-length}</i>	
<i>next-hop-ipaddr</i>	Specifies the next-hop router to use to reach the route destination. The address must be in the same subnet as the ACOS device.
<i>distance</i>	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 <i>partition-name</i> [vrid <i>vrid</i>]	Forwards the traffic to the specified L3V partition as the next hop. The vrid option specifies the VRRP-A VRID, if applicable.
description <i>string</i>	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
<i>seconds</i>	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
<i>seq-num</i>	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 <i>host-src-ipv6addr</i> <i>net-src-ipv6addr</i> / <i>prefix-length</i> object-group <i>name</i>	Source IP address(es) to filter. • any – The ACL matches on all source IP addresses. • host <i>host-src-ipv6addr</i> – The ACL matches only on the specified host IPv6 address. • <i>net-src-ipv6addr</i> /<i>prefix-length</i> – The ACL matches on any host in the specified subnet. • object-group <i>name</i> – The ACL matches on the object group.
eq <i>src-port</i> gt <i>src-port</i> lt <i>src-port</i> range <i>start-src-port end-src-port</i>	For tcp or udp , the source protocol ports to filter. • eq <i>src-port</i> – The ACL matches on traffic from the specified source port. • gt <i>src-port</i> – The ACL matches on traffic from any source port with a higher number than the specified port. • lt <i>src-port</i> – The ACL matches on traffic from any source port with a lower number than the specified port. • range <i>start-src-port end-src-port</i> – The ACL matches on traffic from any source port within the specified range.
any host <i>host-dst-ipv6addr</i> <i>net-dst-ipv6addr</i> / <i>mask-length</i>	Destination IP address(es) to filter.

Parameter	Description
 object-group <i>name</i>	
eq <i>dst-port</i> gt <i>dst-port</i> lt <i>dst-port</i> range <i>start-dst-port end-dst-port</i>	For tcp or udp, the destination protocol ports to filter. • eq <i>dst-port</i> – The ACL matches on traffic from the specified destination port. • gt <i>dst-port</i> – The ACL matches on traffic from any destination port with a higher number than the specified port. • lt <i>dst-port</i> – The ACL matches on traffic from any destination port with a lower number than the specified port. • range <i>start-dst-port end-dst-port</i> – 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 <i>vlan-id</i>	Matches on the specified VLAN. VLAN matching occurs for incoming traffic only.
dscp <i>num</i>	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
<i>ipv6-addr</i>	Valid unicast IPv6 address.
<i>prefix-length</i>	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
<code>redirect</code>	Disables sending of ICMPv6 Redirect messages.
<code>unreachable</code>	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 nat 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
<i>list-name</i>	Name of the source list.
<i>pool-name</i>	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
<i>pool-name</i>	Name of the address pool.
<i>start- ipaddr</i>	Beginning (lowest) IP address in the range.
<i>end- ipaddr</i>	Ending (highest) IP address in the range.
netmask <i>mask- length</i>	Network mask for the IP addresses in the pool, 64-128.
gateway <i>ipv6-addr</i>	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 <i>num</i>	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
<i>pool-group-name</i>	Name of the pool group.
vrid <i>num</i>	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
<i>ipv6-addr</i>	IPv6 unicast address of the neighbor.
<i>macaddr</i>	MAC address of the IPv6 neighbor.
ethernet	Ethernet interface connected to the neighbor.

Parameter	Description
<i>port-num</i>	
trunk <i>trunkID</i>	Trunk interface connected to the neighbor.
tunnel <i>tunnel-num</i>	Tunnel interface connected to the neighbor. You can specify 1-128.
<i>vlan-id</i>	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
<i>list-name</i>	Name of the IP prefix list. The name cannot contain blanks.
description <i>string</i>	Description of the IP prefix list.
seq <i>sequence-num</i>	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 <i>prefix-length</i>	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 <i>prefix-length</i>	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	<code>[no] ipv6 reroute</code>
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	<code>[no] suppress-protocols <i>protocol</i></code>

Parameter	Description
<i>protocol</i>	• <code>connected</code> - Physically connected • <code>ebgp</code> - External Border Gateway Protocol • <code>ibgp</code> - Internal Border Gateway Protocol • <code>isis</code> - Intermediate System to Intermediate System protocol

Parameter	Description
	<code>ospf</code> - Open Shortest Path First protocol <code>rip</code> - Routing Information Protocol <code>static</code> - 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
<i>ipv6addr</i>	IPv6 unicast address of the route destination.
<i>prefix-length</i>	Prefix length, 1-128.
<i>next-hop-ipv6addr</i>	IPv6 unicast address of the next-hop gateway to the destination.
<i>distance</i>	Distance value for the route, 1-255.

Parameter	Description
<i>string</i>	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 <i>AS-num</i>	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 [<i>tag</i>] 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 [<i>tag</i>]	Enter configuration mode for Intermediate System to Intermediate System (IS-IS).
ospf [<i>process-id</i>]	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
<i>num</i>	Administrative distance, 1-255.
<i>ipaddr</i> <i>/mask-length</i>	Network prefix and mask length. The specified distance is applied only to routes with a matching source address.
<i>acl-id</i>	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
<i>acl-id</i> prefix <i>list-name</i>	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.
<i>interface</i>	Interface on which updates are filtered. You can specify the following types of interfaces: <code>ethernet portnum</code> – Ethernet data interface. <code>loopback [num]</code> – Loopback interface. If you do

Parameter	Description
	not specify an interface number, route updates are filtered out on all loopback interfaces. • <code>trunk trunknum</code> – Trunk interface. • <code>ve ve-num</code> – 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
<i>num</i>	Maximum number of RIP routes allowed. You can specify 1-2048.
<i>threshold</i>	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
<i>ipaddr/mask-length</i>	Prefix and mask length of a IPv4 RIP network.
<i>interface</i>	Interface on which to enable RIP. You can specify the following types of interfaces: <code>ethernet portnum</code> – Ethernet data interface. <code>loopback [num]</code> – Loopback interface. If you do not specify an interface number, RIP is enabled on all loopback interfaces. <code>trunk trunknum</code> – Trunk interface. <code>ve ve-num</code> – 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
<i>acl-id</i>	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.
<i>offset</i>	Additional metric to add to routes. You can specify 0-16.
<i>interface</i>	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 [<i>options</i>]	Redistributes route information from Border Gateway Protocol (BGP) into RIP.
connected [<i>options</i>]	Redistributes route information for directly connected networks into RIP.
floating-ip [<i>options</i>]	Redistributes route information for floating IP addresses into RIP.
ip-nat-list [<i>options</i>]	Redistributes routes into RIP for reaching translated NAT addresses allocated from a range list.
ip-nat [<i>options</i>]	Redistributes routes into RIP for reaching translated NAT addresses allocated from a pool.
isis [<i>options</i>]	Redistributes route information from Intermediate System to Intermediate System (IS-IS) into RIP.
lw406 [<i>options</i>]	Redistributes routes into OSPF for Lightweight 4over6. (This is an IPv6 Migration feature.)
ospf [<i>options</i>]	Redistributes route information from Open Shortest Path First (OSPF) into RIP.
static [<i>options</i>]	Redistributes routes into RIP for reaching networks through static routes.
vip [only-flagged only-not-flagged] [<i>options</i>]	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. • <i>options</i> - Optional parameters supported for the options listed above:

Parameter	Description
	• metric <i>num</i> – Metric for the route, 0-16. There is no default. • route-map <i>map-name</i> – 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
<i>update</i>	Amount of time between transmission of RIP route updates to neighbors. You can specify 5-2147483647 seconds. The default is 30 seconds.
<i>timeout</i>	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.
<i>garbage-collection</i>	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
<i>acl-id</i> prefix <i>list-name</i>	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.
<i>interface</i>	Interface on which updates are filtered. You can specify the following types of interfaces: • ethernet <i>portnum</i> – Ethernet data interface. • loopback [<i>num</i>] – Loopback interface. If you do not specify an interface number, route updates

Parameter	Description
	are filtered out on all loopback interfaces. • trunk <i>trunknum</i> – Trunk interface. • ve <i>ve-num</i> – 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
<i>ipv6addr</i>	Link-local IPv6 address of the neighboring IPv6 RIP router.
<i>interface</i>	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
<i>acl-id</i>	ACL that matches on the routes for which to increase the metric.
<i>in</i> <i>out</i>	Direction to which to apply the metric: <i>in</i>— Applies the additional metric value to routes received in updates from RIP neighbors. <i>out</i> – Applies the additional metric value to routes advertised to RIP neighbors.
<i>offset</i>	Additional metric to add to routes. You can specify 0-16.
<i>interface</i>	Interface on which to increase the metric. You can specify the following types of interfaces: <code>ethernet portnum</code> – Ethernet data interface. <code>loopback [num]</code> – Loopback interface. If you do not specify an interface number, the metric is increased on all loopback interfaces.

Parameter	Description
	<code>trunk trunknum</code> – Trunk interface. <code>ve ve-num</code> – 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
<code>[only-flagged only-not-flagged options]</code>	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. • <i>options</i> - 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	<code>[no] route ipv6addr/prefix-length</code> Replace <code>ipv6addr/prefix-length</code> 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
<i>map-name</i>	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.
<i>interface</i>	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
<i>update</i>	Amount of time between transmission of RIP route updates to neighbors. You can specify 5-2147483647 seconds. The default is 30 seconds.
<i>timeout</i>	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.
<i>garbage-collection</i>	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
<i>area-id</i>	Area ID, either an IP address or a number.
access <i>acl-id</i> {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 <i>list-name</i> {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	<pre>[no] area area-id multi-area-adjacency {ethernet portnum loopback num management ve ve-num } neighbor ipaddr</pre>
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
<i>area-id</i>	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
<i>area-id</i>	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	<code>[no] compatible rfc1583</code>
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	<code>[no] distance { num ospf {external inter-area intra-area} num }</code>

Parameter	Description
<i>num</i>	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
<i>num</i>	You can use the <code>ospf</code> 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
<i>acl-id</i>	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 <i>route-type</i>	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
	• <code>ip-nat</code> – Filters advertisement of networks that are translated NAT addresses allocated from a pool. • <code>ip-nat-list</code> – Filters advertisement of networks that are translated NAT addresses allocated from a range list. • <code>ospf [process-id]</code> – Filters advertisement of networks to another OSPF process. • <code>static [only-flagged only-not-flagged]</code> – Filters advertisement of networks reached by static routes. • <code>vip [only-flagged only-not-flagged]</code> – 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: ◦ <code>only-flagged</code> – Redistributes only the VIPs on which the <code>redistribution-flagged</code> command is used. ◦ <code>only-not-flagged</code> – Redistributes all VIPs except those on which the <code>redistribution-flagged</code> 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
<i>ipaddr</i>	IP address of the host.
area <i>area-id</i>	OSPF area where the host is located.
cost <i>num</i>	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
<i>ipaddr</i>	IP address of the OSPF neighbor.
cost <i>num</i>	Specifies the link-state metric to the neighbor, 1-65535. By default, no cost is set.
poll-interval <i>seconds</i>	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 <i>num</i>	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
<i>ipaddr</i> <i>{/mask-length wildcard-mask}</i>	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 <i>area-id</i>	Area ID.
instance-id <i>num</i>	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
<code>cisco</code>	Alternative ABR using Cisco implementation (RFC 3509).
<code>ibm</code>	Alternative ABR using IBM implementation (RFC 3509).
<code>shortcut</code>	Shortcut ABR (draft-ietf-ospf-shortcut-abr-02.txt).
<code>standard</code>	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
<i>max-lsa</i> [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 <i>max-lsa</i> <i>recover-time</i>	Specifies the maximum number of AS-external-LSAs the OSPF router can receive, 0-2147483647. The <i>recover-time</i> option specifies the number of seconds OSPF waits before attempting to recover after <i>max-lsa</i> 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
<i>ipaddr/mask</i>	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
<i>area-id</i>	Area ID, either an IP address or a number.
<i>num</i>	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 <i>area-id</i>	Beginning area ID (either an IP address or a number).
range	Ending area ID.
<i>ipaddr</i>	Subnet address for the range.
<i>/mask-length</i>	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
<i>area-id</i>	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
<i>area-id</i>	Area ID, either an IP address or a number.
<i>ipaddr</i>	IP address of the OSPF neighbor at the other

Parameter	Description
	end of the link.
authentication	Enables authentication on the link.
authentication-key string <i>[string ...]</i>	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 <i>seconds</i>	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 <i>seconds</i>	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 <i>[string ...]</i>	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
<i>process-id</i>	Specifies the IPv4 OSPFv2 process to run on the device, and can be 1-65535.
<i>process-tag</i>	Specifies the IPv6 OSPFv3 process to run on the IPv6 link, and can be 1-65535.
<i>neighbor-id</i>	Router-id of the OSPF device.
<i>neighbor-ip-address</i>	IP address of the interface for the neighboring device.
<i>interface-ip-address</i>	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 <i>num</i>	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 <i>map-name</i>	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
<i>cost</i>	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.
<i>group-num</i>	A specific VRRP-A VRID that will incur the specified <i>cost</i> ; if none are specified, all VRIDs will incur the extra <i>cost</i> . 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
<i>[options]</i>	
ip-nat [<i>ipaddr</i> <i>/mask-length</i> floating-IP-forward-address <i>ipaddr</i>] <i>[options]</i>	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 <i>ipaddr/mask-length</i> option to specify the NAT pool address. The floating-IP-forward-address <i>ipaddr</i> option specifies the forward address to use when redistributing the route to the NAT pool address.
ip-nat-list <i>[options]</i>	Redistributes routes into OSPF for reaching translated NAT addresses allocated from a range list.
isis <i>[options]</i>	Redistributes routes into OSPF for IS-IS.
lw406 <i>[options]</i>	Redistributes routes into OSPF for Lightweight 4over6. (This is an IPv6 Migration feature.)
ospf <i>[process-id]</i> <i>[options]</i>	Redistributes routes into this OSPFv2 process for reaching networks in another OSPFv2 process.
rip <i>[options]</i>	Redistributes routes into OSPF for RIP.
static <i>[options]</i>	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 <i>ipaddr</i> option to specify the

Parameter	Description
address <i>ipaddr</i> { only- flagged only-not- flagged }] [<i>options</i>]	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. • <i>options</i> - 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 <i>num</i> – Metric for the route, 0-16777214. The default is 20. • route-map <i>map-name</i> – Name of a route-map. • tag <i>num</i> – 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
<i>min-delay</i>	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.
<i>max-delay</i>	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 <i>option</i>	Enables distribution of routes from other sources into IS-IS. For available options, see redistribute .
summary-prefix <i>ipv6-</i> <i>addr/prefix</i> [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
<i>string</i>	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 “isis1pwd” 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 isis11pwd 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 <i>name</i> [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	<code>[no] default-information originate</code>
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
<i>num</i>	Specifies the distance, 1-255.
<i>system-id</i>	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
<i>string</i>	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
<code>level-1</code>	Level-1 (intra-area) only.
<code>level-1-2</code>	Level-1 and Level-2.
<code>level-2-only</code>	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 .
<i>seconds</i>	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 <code>lsp-refresh-interval</code> must be smaller than the max-lsp-lifetime .

max-lsp-lifetime

Description	Configure the LSP maximum lifetime.
Syntax	<pre>[no] max-lsp-lifetime seconds</pre> Replace <i>seconds</i> 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 <code>max-lsp-lifetime</code> 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	<pre>[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]}</pre>

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
	• level1-2 – Supports 24-bit SPF calculation only for circuit type Level-2. • level1-1-2 – 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. • level1-1 – Supports both metric lengths only for circuit type Level-1. • level1-2 – Supports both metric lengths only for circuit type Level-2. • level1-1-2 – 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. • level1-1 – Supports 6-bit SPF calculation only for circuit type Level-1. • level1-2 – Supports 6-bit SPF calculation only for circuit type Level-2. • level1-1-2 – 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. • level1-1 – Supports 24-bit SPF calculation only for circuit type Level-1. • level1-2 – Supports 24-bit SPF calculation only for circuit type Level-2. • level1-1-2 – 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. • level1-1 – Supports 6-bit SPF calculation only for circuit type Level-1. • level1-2 – Supports 6-bit SPF calculation only for circuit type Level-2. • level1-1-2 – 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 (**level1-1-2**). For all options that accept the **level1-1**, **level1-1-2**, or **level1-2** keyword, the default is **level1-1**.

Mode IS-IS

net

Description Configure a Network Entity Title (NET) for the instance.

Syntax `[no] net area-address.system-id.00`

Parameter	Description
<i>area-address</i>	Specifies the address of the IS-IS area.
<i>system-id</i>	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
<i>num</i>	specified Ethernet data port.
lif <i>num</i>	Disables routing updates from being sent on the specified logical interface.
loopback <i>num</i>	Disables routing updates from being sent on the specified loopback interface.
trunk <i>num</i>	Disables routing updates from being sent on the specified trunk interface.
ve <i>ve-num</i>	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.
<i>[options]</i>	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 <code>{seconds wait-for-bgp}</code>	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	<code>[no] spf-interval-exp min-delay max-delay [level-1 level-2]</code>

Parameter	Description
level-1 level-2	Specifies the IS-IS level to which to apply the interval setting. The default is <code>level-1</code>.
<i>min-delay</i>	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
<i>max-delay</i>	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
<i>ipaddr</i> <i>/mask-length</i>	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 ipv6`

Parameter	Description
<code>[no] aggregate-address options</code>	See aggregate-address .
<code>[no] auto-summary</code>	See auto-summary .
<code>[no] bgp dampening options</code>	See bgp dampening .
<code>[no] default-information originate</code>	See default-information originate .
<code>[no] distance</code>	See distance .
<code>[no] exit-address-family</code>	Exits the address-family configuration level.
<code>[no] maximum-paths</code>	See maximum-paths .

Parameter	Description
[no] neighbor <i>options</i>	neighbor neighbor-id activate

Parameter	Description
	<u>neighbor neighbor-id advertisement-interval</u>
	<u>neighbor neighbor-id allowas-in</u>
	<u>neighbor neighbor-id as-origination-interval</u>
	<u>neighbor neighbor-id capability</u>
	<u>neighbor neighbor-id collide-established</u>
	<u>neighbor neighbor-id description</u>
	<u>neighbor neighbor-id dont-capability-negotiate</u>
	<u>neighbor neighbor-id ebgp-multihop</u>
	<u>neighbor neighbor-id enforce-multihop</u>
	<u>neighbor neighbor-id fall-over</u>
	<u>neighbor neighbor-id maximum-prefix</u>
	<u>neighbor neighbor-id override-capability</u>
	<u>neighbor neighbor-id passive</u>
	<u>neighbor neighbor-id password</u>
	<u>neighbor neighbor-id peer-group</u>
	<u>neighbor neighbor-id remote-as</u>
	<u>neighbor neighbor-id remove-private-as</u>
	<u>neighbor neighbor-id route-map</u>
	<u>neighbor neighbor-id send-community</u>
	<u>neighbor neighbor-id shutdown</u>
	<u>neighbor neighbor-id soft-reconfiguration</u>
	<u>neighbor neighbor-id strict-capability-</u>

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 <i>options</i>	See network .
[no] redistribute <i>options</i>	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
<i>ipaddr</i> <i>/mask-length</i>	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
<code>as-path</code>	Use the AS path when selecting the best path for a route. AS path consideration is enabled by default.
<code>ignore</code>	Ignore the AS path when selecting the best path for a route.
<code>compare-routerid</code>	Enables comparison of router IDs when comparing identical routes received from different neighbors. In this case, the route from the neighbor with the lowest route ID is selected. By default, BGP receives routes with identical eBGP

Parameter	Description
	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
<i>dampening-options</i>	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. • max-suppress-duration—Specifies the maximum time that a dampened

Parameter	Description
	route is suppressed. You can specify 1-255 minutes. The default is 60 minutes (4 times the half-life time).
<i>map-name</i>	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.
<i>num</i>	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
<code>restart-time</code>	BGP peer graceful restart time in seconds.
<code>stalepath-time</code>	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
<i>num</i>	Count value (0-127).

Mode BGP

bgp router-id

Description Configure the router ID.

Syntax `[no] bgp router-id ipaddr`

Parameter	Description
<i>ipaddr</i>	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
<i>seconds</i>	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
<i>admin-distance ipaddr/mask-length [acl-id]</i>	Overrides the configured administrative distance for specific prefixes. The <i>acl-id</i> 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 <i>external</i> <i>internal</i> <i>local</i>	<i>external</i> – Specifies the administrative distance (1-255) for BGP routes learned from another AS. The default external administrative distance is 20. <i>internal</i> – Specifies the administrative distance (1-255) for BGP routes learned from a neighbor within the same AS. The default internal administrative distance is 200. <i>local</i> – 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
<i>num</i>	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
<i>neighbor-id</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>seconds</i>	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
<i>neighbor-id</i>	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.
<i>occurrences</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: - IPv4 address. - IPv6 address. - Name of a peer group.
<i>seconds</i>	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
<i>neighbor-id</i>	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.
<i>route-refresh</i>	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
<i>neighbor-</i>	ID of the neighbor, which can be one of the following

Parameter	Description
<i>id</i>	types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>map-name</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>string</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>ip-access-list</i>	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
<i>neighbor</i>	The IPv4 or IPv6 address of the neighbor router, or the router tag (1-128 characters).
<i>count</i>	The maximum hop count to reach the neighbor (1-255). If no <i>count</i> 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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>AS-path-access-list</i>	AS path list. To configure an AS path list, use the following command at the global configuration level of the CLI: <pre>ip as-path access-list</pre>
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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: - IPv4 address. - IPv6 address. - Name of a peer group.
<i>num</i>	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.
<i>threshold</i>	Percentage of the allowed maximum at which a warning message is generated. You can specify 1-100. The default is 75 percent.
<i>[restart restart-interval]</i>	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
<i>neighbor-id</i>	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
<i>neighbor-</i>	ID of the neighbor, which can be one of the following

Parameter	Description
<i>id</i>	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
<i>neighbor-id</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>string</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>group-name</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>list-name</i>	Name of the prefix list.
<i>in out</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>AS_num</i>	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
<i>neighbor-</i>	ID of the neighbor, which can be one of the following

Parameter	Description
<i>id</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>map-name</i>	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
<i>neighbor-id</i>	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
<i>neighbor-id</i>	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
<i>neighbor-id</i>	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
<i>neighbor-id</i>	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
<i>neighbor-id</i>	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.
<i>interval</i>	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.
<i>holdtime</i>	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.
<i>seconds</i>	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
<i>neighbor-id</i>	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.
<i>map-name</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: - IPv4 address. - IPv6 address. - Name of a peer group.
<i>source</i>	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
<i>neighbor-id</i>	ID of the neighbor, which can be one of the following types of values: • IPv4 address. • IPv6 address. • Name of a peer group.
<i>num</i>	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
<i>ipaddr</i> <i>/mask-length</i> <i>ipaddr</i>	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: <u><i>ipv6addr/mask-length</i></u>
backdoor	Specify a backdoor BGP route.
community <i>community-list</i>	Match the specified BGP community list.
route-map <i>map-name</i>	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.

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] |
lw406 [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	Redistributes routes into BGP for Lightweight

Parameter	Description
[<i>options</i>]	4over6. (This is an IPv6 Migration feature.)
nat64 [route-map <i>map-name</i>]	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.
ospf [route-map <i>map-name</i>]	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 <i>map-name</i>]	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 <i>map-name</i>] only-not-flagged [route-map <i>map-name</i>] [route-map <i>map-name</i>]]	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.

Parameter	Description
	route-map <i>map-name</i> -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
<i>interval</i>	Specifies the amount of time between transmission of keepalive messages to neighbors. You can specify 0-65535 seconds.
<i>holdtime</i>	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 <code>extended-asn-cap</code> 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 <code>extended-asn-cap</code> 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
<i>seconds</i>	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.
<pre>update- active- vlan {all 13- packet}</pre>	Use this option to update the active VLANs. You can specify one of the following packet types: • <code>all</code> – This option forces the system to update VLAN by any kind of packet (e.g. ARP packet). • <code>13-packet</code> – This option updates the VLAN by 13-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
<code>vlan <i>id</i></code>	Specify the VLAN ID to apply the health check method so that ACOS can detect the active or standby mode of the VLAN.
<code>method</code>	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 16 : Sub-commands in the Ping Method configuration mode

Parameter	Description
interface {ethernet <i>eth-id</i> trunk <i>trunk-</i> <i>id</i> }	Mandatory. Specify the output interface through which the echo request (ping) will be sent. The following interfaces can be specified: • ethernet <i>eth-id</i> - Specify the Ethernet

Table 16 : Sub-commands in the Ping Method configuration mode

Parameter	Description
	interface ID number. • trunk <i>trunk-id</i> - Specify the trunk interface ID number.
interval <i>num</i>	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 <i>ipv4-address</i> {nexthop-mac <i>mac-address</i>	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: <i>aabb.ccdd.eeff</i> or <i>AA:BB:CC:DD:EE:FF</i>.
source-ip <i>ipv4-address</i> {source-mac <i>mac-address</i>	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: <i>aabb.ccdd.eeff</i> or <i>AA:BB:CC:DD:EE:FF</i>. 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 16 : 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 <i>vlan-id</i>	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 17 : Sub-commands in the GARP Method configuration mode

Parameter	Description
interface {eth- ernet <i>eth-id</i> trunk <i>trunk-id</i> }	Mandatory. Specify the interface that will receive GARP packets when the device is in active mode. The following interfaces can be specified: • ethernet <i>eth-id</i> - Specify the Ethernet interface ID number. • trunk <i>trunk-id</i> - Specify the trunk interface ID number.
interval <i>num</i>	Specify the time interval, in seconds, between

Table 17 : 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 <i>ipv4-address</i>	Mandatory. Specify the nexthop IPv4 address of the target device.
standby-interface { ethernet <i>eth-id</i> trunk <i>trunk-id</i> }	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 <i>eth-id</i> - Specify the Ethernet interface ID number. • trunk <i>trunk-id</i> - 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 18 : Sub-commands in the Packet Count Method configuration mode

Parameter	Description
active-threshold <i>num</i>	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 <i>eth-id</i> trunk <i>trunk-id</i> }	Mandatory. Specify the target interface to monitor the packet rate. The following interfaces can be specified: • ethernet <i>eth-id</i> - Specify the Ethernet interface ID number. • trunk <i>trunk-id</i> - Specify the trunk interface ID number.
interval <i>num</i>	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.
13-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 <i>vlan-id</i>	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 18 : 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 pass- ive-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-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 <i>string</i>
	Replace <i>string</i> 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
<i>port-num</i>	Add the specified tagged ethernet port to the VLAN. To add a range of ports, use the to <i>port-num</i> option.
<i>trunk-num</i>	Add the specified tagged trunk to the VLAN. To add a range of trunks, use the to <i>trunk-num</i> 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-PU (PU1 and PU2) based on the source IP address.
dip	Distribute the traffic evenly to the multi-PU (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-PU 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-PU based on the layer 4 source port.
l4-dst-port	Distributes the traffic to the multi-PU 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
<i>port-num</i>	Add the specified untagged ethernet port to the VLAN. To add a range of ports, use the to <i>port-num</i> option.
<i>lif-num</i>	Add the specified logical interface to the VLAN.
<i>trunk-num</i>	Add the specified untagged trunk to the VLAN. To add a range of trunks, use the to <i>trunk-num</i> 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-filter]	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.
<i>ipv4addr ipv4addr /mask- length</i>	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 <code>clear bgp ipv6</code> .
dampening [<i>network</i>]	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 [<i>network</i>]	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.
<i>as-num</i>	Clear all peers with the specified AS number.
<i>ipv4-addr</i>	Clear the specified IPv4 BGP neighbor.
<i>ipv6-addr</i>	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
<i>group-name</i>	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
<i>view-name</i>	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
<i>ipaddr/mask-length</i>	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
<i>ipv6addr/mask-length</i>	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
<i>community-number</i>	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
<i>list-name</i>	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 [<i>community-number</i>] [<i>options</i>]	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 <i>list-name</i> [exact-match]	Displays routes matching the specified community list. The exact-match option displays only the routes that have exactly the same communities.
dampening { <i>options</i> }	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
<i>list-name</i>	list.
inconsistent-as	Displays routes that have inconsistent AS Paths.
large-community <i>num</i>	Displays routes matching the large communities. Large community number in the format XX:YY:ZZ.
large-community-list <i>list-name</i>	Displays routes matching the large community-list.
neighbors [<i>ipv4addr</i> <i>ipv6addr</i> [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 <i>list-name</i>	Displays routes that match the specified prefix list.
quote-regexp <i>string</i>	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: "regexp-string-1").
regexp <i>string</i> [<i>string</i> ...]	Displays routes that match the specified AS-path regular expression(s).

Parameter	Description
route-map <i>map-name</i>	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
<i>process-id</i>	Specifies the OSPFv2 process. If you omit this option, settings for all configured OSPFv2 processes are displayed.
<i>tag</i>	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
<i>process-id</i>	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.
<i>tag</i>	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3

Parameter	Description
	processes are displayed.
<i>ipaddr</i> [detail]	Displays information for the specified neighbor. For detailed information, use the detail option. For summary information, omit the detail option.
<i>all</i>	Includes neighbors whose status is Down. Without this option, down neighbors are not included in the output.
detail [<i>all</i>]	Displays detailed information for all neighbors. To include down neighbors in the output, use the all option.
interface <i>ipaddr</i>	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
<i>process-id</i>	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2

Parameter	Description
	processes are displayed.
<i>tag</i>	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
<i>process-id</i>	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.
<i>tag</i>	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
<i>ipv4addr</i> <i>ipv6addr</i>	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
<code>ipv6addr </code> <code>ipv6addr/mask-length</code>	Network and mask information.
<code>community</code>	Displays routes for communities. Enter the

Parameter	Description
<i>[community-number]</i> <i>[options]</i>	community number in AA:NN format. The following <i>options</i> 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 <i>list-name</i> <i>[exact-match]</i>	Displays routes matching the specified community list. The exact-match option displays only the routes that have exactly the same communities.
dampening { <i>options</i> }	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 <i>list-name</i>	Displays routes that match the specified filter list.
inconsistent-as	Displays routes that have inconsistent AS Paths.
labeled	IPv6 prefix <network>/<length>.
large-community <i>numXX:YY:ZZ</i> 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-community-list <i>list-name</i>	Displays routes matching the large community-list.
neighbors [<i>ipv4addr</i> <i>ipv6addr</i> [<i>options</i>]]	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 <i>list-name</i>	Displays routes that match the specified prefix list.
quote-regexp <i>string</i>	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: "regexp-string-1").
regexp <i>string</i> [<i>string</i> ...]	Displays routes that match the specified AS-path regular expression(s).
route-map <i>map-name</i>	Displays routes that match the specified route map.
summary	Displays a summary of BGP neighbor status.
unicast { <i>ipv6addr</i> <i>ipv6addr/mask-</i>	Displays IPv6 routes for the specified unicast address family. The longer-prefixes option includes prefixes that have a longer mask than

Parameter	Description
<i>length</i> [longer-prefixes]	the one specified.
view <i>view-name</i>	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
<i>ipv6addr</i> <i>ipv6addr/mask-length</i>	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
<i>ipv4addr</i> <i>ipv4addr/mask-length</i>	IPv4 prefix and mask length.
longer-prefixes	Include prefixes that have a longer mask than the one specified.

Mode All

Example This

```
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
<i>view-name</i>	Name of the view.
<i>ipv4addr</i> <i>ipv4addr/mask-length</i>	Prefix and mask.
ipv4 { multicast unicast } summary	Displays information for the specified IPv4 address family.
neighbors [<i>ipv4addr</i> <i>ipv6addr</i>]	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 <i>ipaddr</i>	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 <i>ipaddr</i>	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 0x8000000c9  0xcb72  2
2.2.2.2          2.2.2.2          638 0x800000008  0xdb92  2
3.3.3.3          3.3.3.3         1998 0x8000000cb  0x47c1  2
4.4.4.4          4.4.4.4         1717 0x8000000f6  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 0x800000006  0xec1b
11.0.0.1         3.3.3.3          203 0x800000005  0x14ef
13.0.0.2         4.4.4.4         1717 0x800000006  0xbf3c
14.0.0.1         4.4.4.4         1962 0x800000004  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 0x8000000a3  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 0x80000008e  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
<i>process-id</i>	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 <i>[process-id]</i>	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
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
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
<i>tag</i>	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] <i>ipaddr</i>	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 0x80000000c 0xfa01    1
0.0.0.3        100.1.1.1         31 0x800000001 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 0x80000000d 0x9356    1
0.0.0.0        100.1.1.1         18 0x800000003 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 0x800000001 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 0x800000001 0x5d5f    1
Network-LSA

            AS-external-LSA
```

Link State ID	ADV Router	Age	Seq#	CkSum
0.0.0.4	9.1.1.1	1508	0x800000017	0x6aad E2
0.0.0.1	100.1.1.1	29	0x800000001	0xcd18 E2

show ipv6 ospf topology

Description Display OSPFv3 topology information.

Syntax `show ipv6 ospf [tag] topology [area area-id]`

Parameter	Description
<i>tag</i>	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes is displayed.
area <i>area-id</i>	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]
[11 | 12 | level-1 | level-2]
```

Parameter	Description
<i>tag</i>	Specifies the IS-IS tag (area). If you do not specify a tag value, database entries for all areas is displayed.
<i>lspid</i>	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.
11 12 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
  isisSysStatAttmpToExMaxSeqNums: 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
  isisSysStatAttmpToExMaxSeqNums: 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 <i>port-num</i>	Displays IS-IS information for the specified Ethernet data port.
lif <i>num</i>	Displays IS-IS information for the specified logical interface.
loopback <i>num</i>	Displays IS-IS information for the specified loopback interface.
trunk <i>num</i>	Displays IS-IS information for the specified trunk interface.
ve <i>ve-num</i>	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 <i>id</i>	Displays the health check entry status for the specified VLAN ID.
vlan <i>id</i> 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 | 13-protocol | 14-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.
13-protocol	Layer 3 protocol (ARP, IP, IPv6, IPv6 neighbor/Router).
14-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
<i>plugin-string</i>	Configure the plugin string (1-128 characters).

Parameter	Description
<i>application-string</i>	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 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:

- [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 <i>[host-ip]</i>	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.
<i>host-mac</i>	The MAC address of the overlay host.
vni <i>overlay-segment-id</i>	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 <i>ipv4-address</i>	Specify the source IPv4 address of the VTEP.
local-ipv6-address <i>ipv6-address</i>	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 <i>ipv4-address</i>	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 <i>ipv6-address</i>	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 <i>name</i>	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 <i>Configuring Overlay Networks</i> 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
<code>min-port <i>num</i></code>	Specify the minimum port number. The range can be from 1-65535.
<code>max-port <i>num</i></code>	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 submenu.

Specifies the VNI or VSID of the remote VTEP when used at the Remote VTEP submenu.

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 <i>overlay-segment-id</i>	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 <i>overlay-partition</i>	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 <i>logical-interface-id</i>	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
<code>fragmentation-mode-inner</code>	Enable the inner fragmentation.
<code>gateway-mac</code>	Configures the MAC address for the gateway

Parameter	Description
<i>mac-address</i>	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.
vlan-dest-port <i>port</i>	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
<code>min-port <i>num</i></code>	Specify the minimum port number. The range can be from 1-65535.
<code>max-port <i>num</i></code>	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
<code>encap-table</code>	Displays the IP address of encapsulated endpoints in the overlay tunnel.
<code>vtep [vtep-id statistics]</code>	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 Pkts 0
Reassembled Pkts         0
Host => 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 Pkts 0
In Bad v6 Inner len Pkts 0
```

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 <i>vtep-id</i>	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
<code>aaa-policy</code>	Configure AAM AAA policy configuration.
<code>authentication</code>	Configure AAM authentication related configuration.
<code>authorization</code>	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 Baselineing 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
<code>[no] account</code> <i>account-name-string</i>	Admin account name required to log onto the Active Directory server.
<code>[no] password</code> <i>string</i>	Password required for logging onto the Active Directory server.
<code>[no] realm</code> <i>realm-string</i>	URL of the host realm for the Active Directory server.
<code>[no] service-principal-name</code> <i>string</i>	Name of the account object used for the authentication service instance.
<code>[no] user-tag</code> <i>string</i>	Customized tag.

Default None

Mode Configuration Mode

aam authentication account sampling-enable

Description Enable baselining.

Syntax `[no] authentication account sampling-enable`

Parameter	Description
<code>all</code>	Include all responses.
<code>request-normal</code>	Configure the total normal request.
<code>request-dropped</code>	Configure the total dropped request.
<code>response-success</code>	Configure the total success response.
<code>response-failure</code>	Configure the total failure response.
<code>response-error</code>	Configure the total error response.
<code>response-timeout</code>	Configure the total timeout response.
<code>response-other</code>	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 Configuring JWT template for JWT issuance

Syntax `aam authentication jwt <template-name>`

Command	Description
<code>[no] issuer</code>	Specifying JWT issuer (“iss”) claim value.

Command	Description
[no] action action	Specifying 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 append to URI parameter.
[no] signature-secret secret	Specifying the secret to sign the JWT signature.
[no] token-lifetime seconds	Specifying the valid duration of the JWT when it is generated.

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
<code>form-based</code>	Configure form-based authentication logon.
<code>http-authenticate</code>	Configure HTTP-authenticate logon.

Default None

Mode Configuration 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
<code>[no] action-url <i>url-string</i></code>	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: <i>/url-string</i>
<code>[no] authz-failure-message <i>string</i></code>	Specify authorization failure message shown in logon page.
<code>[no] captcha-variable <captcha_var_name></code>	Specify the variable name of CAPTCHA token used in the logon form.
<code>[no] challenge-variable</code>	Specify a challenge variable name on the form submission.
<code>[no] changepassword-url <i>string</i></code>	URL for the POST action to be performed by the client browser after the end-user enters their expired and new credentials.
<code>[no] csp-support {none self sepcificURI}</code>	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).

Parameter	Description
	specificURI—Sets customized CSP frame-ancestors (maximum 2 URIs can be set). Examples for URI, <pre>https://a.example.com</pre> <pre>https://b.example.com</pre>
[no] disable-change-password-link <i>string</i>	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 <i><second></i>	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] login-failure-message <i>string</i>	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 <i>string</i>	Specify the new-pin variable name used when the form is submitted.
[no] next-token-variable <i>string</i>	Specify the next-token variable name used when the form is submitted.
[no] notifychange-password-change-url <i>string</i>	URL for the POST action to be performed by the client browser after the end-user saves the new credentials.
[no]	URL for the POST action to be performed

Parameter	Description
notifychangepassword-continue-url <i>string</i>	by the client browser after the end-user confirms the password change.
[no] passcode-variable <i>string</i>	Name of the data field for the passcode entered into the logon form by the end-user.
[no] password-variable <i>string</i>	Name of the data field for the password entered into the logon form by the end-user.
[no] portal default-portal or [no] portal <i>name</i> logon <i>name</i> failpage <i>name</i> changepasswordpage <i>name</i> {new-pin-page <i>name</i> next-token-page <i>name</i> challenge-page <i>name</i> }	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 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 <i>num</i>	Number of times ACOS will resend the

Parameter	Description
	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 <i>num</i> <i>account-lock</i>	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 <i>string</i>	Customized user tag.
[no] username-variable <i>string</i>	Name of the data field for the username entered into the logon form by the end-user.
[no] changepassword-username-variable <i>string</i>	Name of the data field for the username entered into the change-password form by the end-user.
[no] changepassword-old-password-variable <i>string</i>	Name of the data field for the old password entered into the change-password form by the end-user.
[no] changepassword-new-password-variable <i>string</i>	Name of the data field for the new password entered into the change-password form by the end-user.
[no] changepassword-password-confirm-variable <i>string</i>	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-logout profiles. When you create one for form-based login, 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
<code>[no] secret-key <key></code>	Server secret key used when verifying the CAPTCHA token.
<code>[no] url <api_url></code>	API URL used for CAPTCHA verification. The scheme should be HTTP or HTTPS.
<code>[no] method {POST GET}</code>	HTTP method that API URL uses; default is POST. This option will be always displayed on CLI.
<code>timeout {1..255}</code>	Timeout value when waiting for response. The range is from 1 to 255 seconds, default is 10 seconds.
<code>secret-key-param-name <param_name></code>	Parameter name of secret-key used in CAPTCHA API verification.
<code>token-param-name <param_name></code>	Parameter name of token used in CAPTCHA API verification.
<code>resp-result-field-name <field_name></code>	Response result field name.
<code>resp-error-msg-field-name <field_name></code>	Field name of error message in the CAPTCHA JSON response
<code>send-client-ip param-name <field_name></code>	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
<pre>[no] auth- method { basic { challenge- response-form <i>name</i> challenge- page <i>name</i> challenge- variable <i>name</i> / new-pin- page <i>name</i> next- token-page <i>name</i> new-pin- variable <i>name</i> next- token- variable <i>name</i> / enable / realm <i>name</i>} / negotiate</pre>	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 ◦ 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.

Parameter	Description
enable / }	
[no] hsts-support timeout <i><second></i>	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-template <i>string</i>	Specify name of the packet capture template to bind with this object.
[no] retry <i>num</i>	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 <i>num</i>	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
<code>change-password</code>	Change the password page configuration. The following commands are available after you enter <code>change-password</code>: • action-url— Specify the form action URL in the default change password page (1-63 characters). The default is <code>/change.fo</code>. • background <code>{color color file name}</code>— 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 <code>a10bg.gif</code>. • confirm-password — Configure the confirm password text on the default change password page. Specify at least one of the following: • color <code>color</code> - name or hex value for the desired font color. • font <code>font-name</code> - font type to use for the text. Type <code>font ?</code> to see the list of available fonts. • size <code>size</code> - size of the font (1-7). • text <code>string</code> - text you want to use on the page (1-63 characters). • confirm-password-var - Configure the confirm password variable name on the

Parameter	Description
	default change password page (1-63 characters). The default is <code>cp_cfm_pwd</code>. • 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 <code>cp_new_pwd</code>. • old-password - Configure the old password text on the default change password page. 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 <code>cp_old_pwd</code>. • 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

Parameter	Description
	(above). username-var - Configure the username variable name on the default change password page (1-63 characters). The default is <code>cp_usr</code>.
logo <i>filename</i> [height <i>num</i>] [width <i>num</i>]	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 enter logon: action-url— Specify the form action URL (1-63 characters). The default is <code>/logon.fo</code>. background {color <i>color</i> file <i>name</i>}— Configure the background on the logon page. You can specify a color, either by name or hex value, or use a .BMP .GIF .JPG, or .PNG file to use for the background. The default is <code>def_bg.gif</code>. When using an image file, 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 <i>color</i> - name or hex value for the desired font color.

Parameter	Description
	◦ font <i>font-name</i> - font type to use for the text. Type font ? to see the list of available fonts. ◦ size <i>size</i> - size of the font (1-7). ◦ text<i>string</i> - 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." • passcode-var - Configure the passcode variable name on the logon page (1-63 characters). The default is <i>passcode</i>. • 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 <i>pwd</i>. • 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 <i>user</i>.

Parameter	Description
<code>logon-fail</code>	Configure the login failed page for the default portal. The following commands are available after you enter <code>logon-fail</code>: • background {<code>color color</code> <code>file name</code>}- 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 <code>a10bg.gif</code>. • background {<code>color color</code> <code>file name</code>}- 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 <code>a10bg.gif</code>. ◦ color <code>color</code> - name or hex value for the desired font color. ◦ font <code>font-name</code> - font type to use for the text. Type <code>font ?</code> to see the list of available fonts. ◦ size <code>size</code> - size of the font (1-7). ◦ text <code>string</code> - 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 <code>fail-msg</code> (above), except that there is no default text string.
<code>notify-change-password</code>	Password change notification page configuration. The following commands are available after you enter <code>notify-change-password</code>: background {<code>color color</code> <code>file name</code>}- Configure the background on the default change

Parameter	Description
	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 <code>a10bg.gif</code>. 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 <code>/notify_change.fo</code>. confirm-password - Configure the confirm password text on the default change password notification page. Specify at least one of the following: • color <i>color</i> - name or hex value for the desired font color. • font <i>font-name</i> - font type to use for the text. Type font ? to see the list of available fonts. • size <i>size</i> - size of the font (1-7). • text <i>string</i> - 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 <code>cp_cfm_pwd</code> • confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is

Parameter	Description
	- confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is <code>cp_cfm_pwd</code> - confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is <code>cp_cfm_pwd</code> - confirm-password-var - Configure the confirm password variable name on the default change password notification page (1-63 characters). The default is <code>cp_cfm_pwd</code> - old-password - Configure the old password text on the default change password notification page. The sub-options are the same as <code>confirm-password</code> (above) - old-password - Configure the old password text on the default change password notification page. The sub-options are the same as <code>confirm-password</code> (above) - old-password - Configure the old password text on the default change password notification page. The sub-options are the same as <code>confirm-password</code> (above) - old-password - Configure the old password text on the default change password notification page. The sub-options are the same as <code>confirm-password</code> (above)
enable-CAPTCHA type {reCAPTCHA v2- checkbox 	Enable Google <code>reCAPTCHA</code> 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

Parameter	Description
reCAPTCHA-v2-invisible reCAPTCHA-v3 site-key <key>	only available when using reCAPTCHA-v2. • reCAPTCHA-size {normal compact} - Size of the widget. The default size is normal. This option is only available when using reCAPTCHA-v2. • reCAPTCHA-size {normal compact} - Size of the widget. The default size is normal. This option is only available when using reCAPTCHA-v2. • reCAPTCHA-size {normal compact} - Size of the widget. The default size is normal. This option is only available when using reCAPTCHA-v2. 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.
ntlm	Configure NTLM 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
<pre>[no] request-uri {equals contains starts-with ends- with} uri</pre>	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 <code>request-uri</code> command: • <code>[no] action-uri <i>uri</i></code> - Specify the action-URI. • <code>[no] domain-variable <i>domain-var</i></code> - Specify domain variable name • <code>[no] header cookie <i>cookie-string</i></code> - Specify new header content in the POST packet by specifying a new cookie in POST packet. • <code>[no] max-packet-collect-size <i>bytes</i></code> - Specifies the number of bytes reserved for response packet

Sub-commands	Sub-command Description and Syntax
	collection in bytes. The default is 1MByte. • <code>[no] other-variables other-var</code> - Specify other variables (<code>n1=v1&n2=v2</code>) in form relay. • <code>[no] password-variable pw-var</code> - Specify password variable name. • <code>[no] user-variable username-var</code> - Specify the username variable name.
<code>[no] sampling-enable</code> <code>[all] [request]</code> <code>[invalid_srv_rsp]</code> <code>[post_fail] [invalid_cred]</code> <code>[bad_req] [not_fnd]</code> <code>[error] [other_error]</code>	Enables baselining the specified relayed message counters. See the “Enabling Baselining and Rate Calculation” topic in the <i>Command Line Interface Reference</i> for an explanation of baselining. • <code>all</code> - all message types. • <code>request</code> - requests • <code>invalid_srv_rsp</code> - “Invalid Server” responses • <code>post_fail</code> - “Post Failed” responses • <code>invalid_cred</code> - “Invalid Credentials” responses • <code>bad_req</code> - “Bad Found” responses

Sub-commands	Sub-command Description and Syntax
	• <code>not_fnd</code> - “Internal Server Error” responses • <code>error</code> - “Bad Request” responses • <code>other_error</code> - “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
<code>domain</code> <i>domain-name</i>	Specify the user domain.
<code>domain-format</code> <code>{user-</code>	Specify the format to use for appending the domain to the credential:

Parameter	Description
principal-name down-level-logon-name	user-principal-name - Append the domain using the User Principal Name format (for example: <i>user@domain</i>). down-level-logon-name - Append the domain using the Down Level Logon Name format (for example: <i>domain\user</i>). 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 <i>name</i> [...]	Kerberos admin account name required to logonto the KDC.
[no] kerberos-kdc { <i>hostname</i> <i>ipaddr</i> }	Hostname or IP address of the KDC.
[no] kerberos-kdc-service-	Name of the service group for multiple KDC servers configured in AAM (under authentication server).

Parameter	Description
group <i>{auth_ service_ group}</i>	
[no] kerberos-realm <i>realm-string</i>	Name of the Kerberos realm secured by the AAA servers.
[no] password <i>string</i>	Password required for logging onto the KDC.
[no] port <i>port-num</i>	Protocol port number on which the KDC listens for requests. The default port is 88.
[no] timeout <i>seconds</i>	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	Specify the backend server assertion

Parameter	Description
<code><URI></code>	consuming service URI
<code>[no] server-login-uri <uri></code>	Specify the URI to trigger the SAML relay.
<code>[no] server-cookie-name <name></code>	Specify the cookie name that used by backend server for authenticated users. Then Thunder will trigger the relay when the cookie is missing.
<code>relay-state value <string> request-uri get-from-backend</code>	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 • 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
<code>[no] application-server {sharepoint exchange-owa}</code>	Specify the type of application server:

Parameter	Description
	• sharepoint - Microsoft Sharepoint • exchange-owa - Microsoft Exchange The default is Microsoft sharepoint.
[no] authentication-uri <i>uri-name</i>	Specify WS-Federation relay URI. The default URI is <code>/_trust/</code>.

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
<pre>[no] SP-initiated-single-logout-service location</pre>	Decide the endpoint of SP-initiator Single Logout (SLO) service. Specify the location of the SP-initiator SLO (for example, /Logout).
<pre>[no] acs-uri-bypass</pre>	After user is authenticated, bypass requests with assertion-consuming-service location URI.
<pre>[no] adfs-ws-federation enable</pre>	Enable ADFS WS_Federation.
<pre>[no] artifact-resolution-service index index-num location string binding soap</pre>	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

Parameter	Description
	artifact resolution service.
[no] assertion-consuming-service index <i>index-num</i> location <i>string</i> 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-redirect-url <i>Name</i>	Specify a URL to redirect. You can specify a string of 1-127 characters.
[no] certificate <i>filename</i>	The SAML service provider certificate file (1-63 characters).
[no] entity-id <i>id</i>	The SAML service provider entity ID (1-63 characters).
[no] metadata-export-service location <i>uri</i> [sign-xml]	The SAML service provider metadata export service. The default location is <code>/A10SP_Metadata</code>. 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.

Parameter	Description
<code>[no] require-assertion-signed enable</code>	Require SAML assertion to be signed.
<code>[no] saml-request-signed disable</code>	Signing SAML requests (AuthnRequest or Artifact Resolve).
<code>[no] sampling-enable</code>	Enables baselining the specified message counters. See the “Enabling Baselining and Rate Calculation” topic in the <i>Command Line Interface Reference</i> for an explanation of baselining.
<code>[no] service-url url</code>	SAML service provider service URL (for example, <code>https://www.a10networks.com/saml.sso</code>).
<code>[no] signature-algorithm {SHA1 SHA256}</code>	Specify SAML request signature algorithm
<code>[no] single-logout-service {post redirect soap}</code>	The SAML service provider single logout service configuration. Specify the location of the single logout service (for example, /SAML/POST), and the binding: • <code>post</code> - POST binding of the single logout service. • <code>redirect</code> - Redirect binding of the single logout service. • <code>soap</code> - SOAP binding of the single logout service.
<code>[no] soap-tls-certificate-validate</code>	Verify the IDP certificate when you establish the TLS connection to IDP for Artifact resolution.
<code>[no] username-attribute</code>	Specify a username to identify and differentiate individual users within the

Parameter	Description
<i>username</i>	database. You can specify a string of 1-63 characters.
user-tag <i>tag-name</i>	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
ldap	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 <i>string</i>	The Distinguished Name (DN) of the LDAP admin account that is required to access the server (1-127 characters).
[no] admin-secret <i>string</i>	Admin password (1-128 characters).
[no] auth-type	LDAP authentication server type (active directory or open LDAP).
[no] base <i>string</i>	LDAP server's search base (1-127 characters).
[no] bind-with-dn	DN must be used for LDAP binding.
[no] default-domain <i>domain-name</i>	Default domain for LDAP (1-63 characters).
[no] derive-bind-dn username-attr <i>attr-name</i>	Derive Distinguished Name for binding from server. Specify the attribute name of username (1-31 characters).
[no] dn-attribute <i>attr-name</i>	Specify Distinguished Name attribute (1-31 characters). The default is cn .
[no] health-check <i>mon-name</i>	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 { <i>hostname</i> <i>ipaddr</i> }	Hostname or IP address of the LDAP server.

Parameter	Description
[no] port <i>port-num</i>	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 <i>seconds</i>	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 <i>string</i>	The type of connection to be used by ACOS when querying the LDAP directory server for user 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 <u>protocol</u> is set to <i>ldaps</i> or <i>starttls</i> .
[no] timeout <i>seconds</i>	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.

Parameter	Description
<code>[no] ldaps-conn-reuse-idle-timeout seconds</code>	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 ocsdp

Description Configure an authentication-server profile for an Online Certificate Status Protocol (OCSP) server.

Syntax `[no] aam authentication server ocsdp profile-name`

This command changes the CLI to the configuration level for the profile, where the following commands are available:

Parameter	Description
<code>[no] health-check <i>mon-name</i></code>	Check the server's health check status. Specify the name of an existing health check monitor (1-63 characters).
<code>[no] health-check-disable</code>	Disable the configured health check configuration.
<code>[no] port-health-check <i>mon-name</i></code>	Check the port's health check status. Specify the name of an existing health check monitor (1-63 characters).
<code>[no] port-health-check-disable</code>	Disable the configured port health check configuration.
<code>[no] responder-ca</code>	

Parameter	Description
[no] responder-cert	The trusted OCSP responder's certificate filename.
[no] url <i>url-string</i>	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 <i>port-num</i>	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 <i>mon-name</i>	Check the server's health check status. Specify the name of an existing health check monitor

Parameter	Description
	(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. 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 <i>protocol</i>	Specifies an enabled authentication protocol. The user can choose among the following: • kerberos-port <i>value</i> –Specify the Kerberos port, default is 88. • kerberos-validate-kdc - Enable validation for the Kerberos KDC server port. • health-check <i>string</i> –Specify a previously configured health monitor for running health checks on the Kerberos KDC server port. • health-check-disable –Disable a configured health check for the Kerberos KDC server port. • kerberos-password-change-port <i>value</i> - Specify the password to change the Kerberos port. Default is 464.
[no] health-check <i>mon-name</i>	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 { <i>hostname</i> <i>ipaddr</i> }	Hostname or IP address of the Windows server.
[no] realm <i>realm-name</i>	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.

Parameter	Description
[no] timeout <i>value</i>	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 <i>profile-name</i>	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 <i>profile-name</i>	Binds servers as members of the configured service-group.
[no] method <i>type</i>	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
<i>template-name</i>	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
<code>[no] account <i>name</i></code>	Specify the name of an AD account (1-63 characters).
<code>[no] accounting-server <i>name</i></code>	Specify the name of a RADIUS accounting server.
<code>[no] accounting-service-group <i>name</i></code>	Specify the name of an authentication service group for RADIUS accounting. This service group can only contain RADIUS servers.
<code>[no] auth-sess-mode {cookie-based ip-based}</code>	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.
<code>[no] cookie-domain <i>domain</i></code>	Specify the domain scope for authentication (for example, <code>.exampledomain.com</code>).
<code>[no] cookie-domain-group <i>id</i></code>	Specify the group ID (1-31 characters) to join in the specified <code>cookie-domain</code> .
<code>[no] cookie-</code>	Enable the cookie httponly attribute

Parameter	Description
httponly-enable	
[no] cookie-max-age <i>seconds</i>	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-samesite <i>strict/lax/none</i>	Specify the value of SameSite attribute for AAM cookie NOTE: <u>Set one of the option strict, lax, or none.</u>
[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 <code>logout-url</code> must first be configured before you can use this option.
[no] log	Enable or disable authentication logs for this template.
[no] login <i>profile-name</i>	Name of a configured authentication login profile.
[no] logout-idle-timeout <i>seconds</i>	Maximum amount of time an authenticated end-user session can be idle before being terminated by ACOS. You can specify 1-86400 seconds.

Parameter	Description
	The default is 300 seconds (5 minutes).
[no] logout-url <i>url-string [...]</i>	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 <i>hostname</i>	Configure hostname for transparent-proxy authentication. The hostname can be 1-31 in length.
[no] relay <i>profile-name</i>	Name of a configured authentication-relay profile.
[no] saml-idp <i>idp-name</i>	Name of the SAML identity provider (1-63 characters).
[no] saml-sp <i>sp-name</i>	Name of the SAML service provider (1-63 characters)
[no] server <i>profile-name</i>	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 <i>group-name</i>	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>	chain - This option is mutual exclusively with server and service-group. server-name - Name of the server.

Parameter	Description
service-group <sg-name>} priority <1-5>	• 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
<code>[no] attribute attr-num {attr-name A10-AX-AUTH-URI} attr-type type operator attr-value</code>	Configure authorization attribute values. • <i>attr-num</i> - Attribute number, 1-32. • <i>attr-name</i> - Attribute name, either a custom name or A10-AX-AUTH-URI. • attr-type <i>type</i> - Data type of the attribute: ◦ integer ◦ ip-addr

Parameter	Description
	◦ string • <i>operator</i> – 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 <i>type</i> differ depending on the type.) • <i>attr-value</i> – Value to be compared.
[no] attribute-rule <i>attr-num</i> { and or } <i>attr-num</i> ...	Rule for combining multiple attributes.
[no] forward-policy-authorize-only	Configure the policy to provide only server information for forward policy feature.
[no] server <i>profile-name</i>	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 <i>group-name</i>	Name of a configured service group of authorization servers.
[no] attribute {1..32} <attr_	Attribute type <i>number</i> which

Parameter	Description
name> attr-type number {equal not-equal less-than more-than less-than-equal-to more-than-equal-to} <num>	supports decimal representation. If the CAPTCHA JSON response has multiple levels. To check the attribute <code>action</code> , set the attribute name to <code>tokeninfo.action</code> .

Default Not set

Mode Configuration Mode

aam jwt-authorization

Description Configuring JWT authorization template which can bind to **AAM authorization policy**

Syntax `aam jwt-authorization <template-name>`

Command	Description
[no] exp-claim-required	Specifying the exp claim, which is required for the JWT authorization.
[no] jwt-cache-enable	Enabling the caching authorized JWT and skip verification and authorization for cached tokens.
[no] jwt-exp-default <i>seconds</i>	Specifying the default token expiration, if exp claim is not available (default 1800).
[no] jwt-forwarding	Specifying the JWT is not stripped, while forwarding the client request.
[no] log-level <i>level</i>	Specifying the JWT authorization syslog level (default value is 1) 0 = Log disable 1 = Only log authorization fail (default) 2 = Only log authorization success 3 = Log all

Command	Description
[no] verification-cert <i>certificate-file</i>	Specifying the certificate to verify JWT signature.
[no] verification-jwks <i>jwks-files</i>	Specifying the jwks file to verify JWT signature.
[no] verification-secret <i>secret</i>	Specifying secret for verify 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
<code>client-id</code> <code><NAME></code>	Specify oauth client-id.
<code>client-secret</code> <code><NAME></code>	Specify oauth client secret for client.
<code>grant-type</code> <code><implicit </code> <code>authorization-</code> <code>code hybrid></code>	Specify oauth client grant type.
<code>parameter-</code> <code>nonce-enable</code>	Enable nonce parameter for authorization and token request.
<code>redirection-</code> <code>endpoint <NAME></code>	OAuth client redirection endpoint service URL, this URL adds /js automatically when authorization-endpoint using GET method.
<code>scope <NAME></code>	Specify request scope parameters (e.g. profile email address phone).
<code>session-init-ttl</code> <code><1-60></code>	TTL for Thunder to wait for first response from authorization server.
<code>token-lifetime <1-</code> <code>2592000 </code> <code>infinity></code>	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.
<code>type <openid-</code> <code>connect></code>	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
<code>relay-type <access-token id-token></code>	Specify token to relay in bearer schema.
<code>relay-uri <all equals contains starts-with ends-with> <NAME></code>	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 mode:

```
ACOS(config)# aam aaa-policy policyname
```

```
ACOS(config-aaa policy:polycyname)# aaa-rule 255  
ACOS(config-aaa policy:polycyname-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 polycyname  
ACOS(config-aaa policy:polycyname)# aaa-rule 255  
ACOS(config-aaa policy:polycyname-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-tmpl-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-tmpl-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 <i>hostname</i> .
ends-with	Match HOST if the request HTTP HOST header ends with the specified <i>hostname</i> .
equals	Match HOST if the request HTTP HOST header is the same as the specified <i>hostname</i> .
starts-with	Match HOST if the request HTTP HOST header starts with the specified <i>hostname</i> .
<i>hostname</i>	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:polycname)# aaa-rule 255
ACOS(config-aaa policy:polycname-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 polycname
ACOS(config-aaa policy:polycname)# aaa-rule 255
ACOS(config-aaa policy:polycname-aaa rule:...)# match-
encoded-uri
```

port

Description Specify a port to match for the AAA rule.

Syntax `[no] port portnum`

Parameter	Description
<i>portnum</i>	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.
<i>uri-string</i>	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	<code>clear aam authentication session kcache [kerberos-relay-name]</code>
Mode	Privileged EXEC and all configuration levels.

clear aam authentication rdns

Description	Clear Reverse DNS entries from ACOS AAM authentication cache table.
Syntax	<code>clear aam authentication rdns {all ipv4 ipv4_addr ipv6 ipv6_addr}</code>
Mode	Privileged EXEC and all configuration levels.

clear aam authentication service-group

Description	Clear authentication service-group statistics.
Syntax	<code>clear aam authentication service-group {all group-name}</code>
Mode	Privileged EXEC and all configuration levels.

clear aam authentication session

Description	Clear authentication session table entries.
Syntax	<code>clear aam authentication session all</code>
	or
Syntax	<code>clear aam authentication session source-addr {ipv4 ipv4-addr ipv6 ipv6-addr}</code>

```
[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	<code>clear aam authentication statistics jwt [name]</code>
Default	NA
Mode	Privileged EXEC and all configuration levels.

clear aam authorization jwt cache

Description	Clear cached JWTs
Syntax	<code>clear aam authorization jwt cache [audience name]</code>
Default	NA
Mode	Privileged EXEC and all configuration levels

clear aam authentication saml idp status

Description	Clear SAML Identity Provider status.
Syntax	<code>clear aam authentication saml idp status</code>
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
<code>rdns</code>	Show RDNS records.
<code>name</code>	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	<code>show aam authentication jwks</code>
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	<code>show aam authentication klist [relay-profile-name]</code> Replace <i>relay-profile-name</i> 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 <i>server-name</i> 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 OCSF 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 <i>partition-name</i>	Shows authentication service group settings for the specified L3V partition only.
brief	Shows brief service group information.
config	Shows service group configuration information.
<i>sg-name</i>	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
<code>aaa-policy</code>	Shows authentication, authorization, and accounting (AAA) policy statistics.
<code>aaa-rule</code>	Shows AAA rule statistics.
<code>form-based-relay</code>	Shows authentication form-based relay statistics.
<code>http-basic-relay</code>	Shows authentication HTTP basic relay statistics.
<code>kerberos-relay</code>	Shows authentication Kerberos relay statistics.
<code>ldap</code>	Shows authentication LDAP statistics
<code>negotiate-kerberos</code>	Shows authentication Kerberos statistics of HTTP negotiate.
<code>ocsp</code>	Shows authentication OCSP server statistics.
<code>ocsp-stapling</code>	Shows authentication OCSP stapling statistics

Parameter	Description
<code>radius</code>	Shows authentication Radius statistics.
<code>saml-sp</code>	Shows SAML service provider statistics.
<code>windows-kerberos</code>	Shows authentication Windows Server Kerberos statistics.

[Table 19](#) describes the fields in this command's output.

Table 19 : 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 19 : 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 19 : 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 19 : 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 19 : 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.