Command Line Interface Reference

AX Series Advanced Traffic Manager

Document No.: D-030-01-00-0003

Ver. 2.6.6-GR1 5/8/2013

Headquarters

A10 Networks, Inc.
3 West Plumeria Dr.
San Jose, CA 95134

Tel: 408 325 8668 (main)
Tel: 408 325 8676 (support)
Fax: 408 325 8666

www.a10networks.com

Information in this document is subject to change without notice.

Trademarks

A10 Networks, A10 Thunder, vThunder, the A10 logo, aACI, aCloud, ACOS, aDCS, aDNS, aELB, aFleX, aFlow, aGalaxy, aPlatform, aUSG, aVCS, aWAF, aXAPI, IDAccess, IDSENTRIE, IP to ID, SmartFlow, SoftAX, Thunder, Unified Service Gateway, Virtual Chassis, VirtualADC, and VirtualN are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners.

Patents Protection

A10 Networks products including all AX Series products are protected by one or more of the following US patents and patents pending: 20120216266, 20120204236, 20120179770, 20120144015, 20120084419, 20110239289, 20110093522, 20100235880, 20100217819, 20090049537, 20080229418, 20080148357, 20080109887, 20080040789, 20070283429, 20070282855, 20070271598, 20070195792, 20070180101, 8387128, 8332925, 8312507, 8291487, 8266235, 8151322, 8079077, 7979585, 7716378, 7675854, 7647635, 7552126

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.

A10 Networks Inc. Software License and End User Agreement

Software for all A10 Networks products contains trade secrets of A10 Networks and its subsidiaries and Customer agrees to treat Software as confidential information.

Anyone who uses the Software does so only in compliance with the terms of the End User License Agreement (EULA), provided later in this document or available separately. Customer shall not:

1) reverse engineer, reverse compile, reverse de-assemble or otherwise translate the Software by any means

2) sublicense, rent or lease the Software.

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks 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 for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' 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 location, which can be found by visiting www.a10networks.com.

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING A10 NETWORKS OR A10 NETWORKS PRODUCTS, OR SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

A10 NETWORKS IS WILLING TO LICENSE THE PRODUCT TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN A10 NETWORKS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

The following terms of this End User License Agreement ("Agreement") govern Customer's access and use of the Software, except to the extent there is a separate signed agreement between Customer and A10 Networks governing Customer's use of the Software

License. Conditioned upon compliance with the terms and conditions of this Agreement, A10 Networks Inc. or its subsidiary licensing the Software instead of A10 Networks Inc. ("A10 Networks"), grants to Customer a nonexclusive and nontransferable license to use for Customer's business purposes the Software and the Documentation for which Customer has paid all required fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the product or products and made available by A10 Networks in any manner (including on CD-Rom, or on-line).

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in or for execution on A10 Networks equipment owned or leased by Customer and used for Customer's business purposes.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and A10 Networks retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of A10 Networks, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

a. transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand A10 Networks equipment

b. make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same

c. reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction

d. disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of A10 Networks. Customer shall implement reasonable security measures to protect such trade secrets.

Software, Upgrades and Additional Products or Copies. For purposes of this Agreement, "Software" and “Products” shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware and hardware, as provided to Customer by A10 Networks or an authorized A10 Networks reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by A10 Networks or an authorized A10 Networks reseller.

OTHER PROVISIONS OF THIS AGREEMENT:

a. CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES

b. USE OF UPGRADES IS LIMITED TO A10 NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LEASEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED

c. THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement.

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation.

Trademarks

A10 Networks, A10 Thunder, vThunder, the A10 logo, aACI, aCloud, ACOS, aDCS, aDNS, aELB, aFleX, aFlow, aGalaxy, aPlatform, aUSG, aVCS, aWAF, aXAPI, IDAccess, IDSENTRIE, IP to ID, SmartFlow, SoftAX, Unified Service Gateway, Virtual Chassis, VirtualADC, and VirtualN are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners.

Patents Protection

A10 Networks products are protected by one or more of the following US patents and patents pending: 20120216266, 20120204236, 20120179770, 20120144015, 20120084419, 20110239289, 20110093522, 20100235880, 20100217819, 20090049537, 20080229418, 20080148357, 20080109887, 20080040789, 20070283429, 20070282855, 20070271598, 20070195792, 20070180101, 8387128, 8332925, 8312507, 8291487, 8266235, 8151322, 8079077, 7979585, 7716378, 7675854, 7647635, 7552126

Limited Warranty

Disclaimer of Liabilities. REGARDLESS OF ANY REMEDY SET FORTH FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL A10 NETWORKS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE PRODUCT OR OTHERWISE AND EVEN IF A10 NETWORKS OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall A10 Networks’ or its suppliers' or licensors' liability to Customer, whether in contract, (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whetherCustomer has accepted the Software or any other product or service delivered by A10 Networks. Customer acknowledges and agrees that A10 Networks has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The Warranty and the End User License shall be governed by and construed in accordance with the laws of the State of California, without reference to or application of choice of law rules or principles. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. This Agreement constitutes the entire and sole agreement between the parties with respect to the license of the use of A10 Networks Products unless otherwise supersedes by a written signed agreement.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid A10 Networks Regular and Technical Support service contracts, the A10 Networks Technical Assistance Center provides support services online and over the phone.

Corporate Headquarters

A10 Networks, Inc.
3 West Plumeria Dr
San Jose, CA 95134 USA

Tel: +1-408-325-8668 (main)
Tel: +1-888-822-7210 (support – toll-free in USA)
Tel: +1-408-325-8676 (support – direct dial)
Fax: +1-408-325-8666

www.a10networks.com

Collecting System Information

The AX device provides a simple method to collect configuration and status information for Technical Support to use when diagnosing system issues.

To collect system information, use either of the following methods.

Using the GUI (Recommended)

1. Log into the GUI.
2. On the main page (Monitor Mode > Overview > Summary), click 🛟 . This option downloads a text log file.
3. Email the file as an attachment to support@A10Networks.com.

Using the CLI

1. Log into the CLI.
2. Enable logging in your terminal emulation application, to capture output generated by the CLI.
3. Enter the **enable** command to access the Privileged EXEC mode of the CLI. Enter your enable password at the Password prompt.

4. Enter the **show techsupport** command.
5. After the command output finishes, save the output in a text file.
6. Email the file as an attachment to support@A10Networks.com.

Note: As an alternative to saving the output in a log file captured by your terminal emulation application, you can export the output from the CLI using the following command:

```
show techsupport export [use-mgmt-port] url
```

(For syntax information, see the *AX Series CLI Reference*.)

About This Document

This document describes features of the A10 Networks AX Series.

FIGURE 1 AX 5630 (front panel view)

Information is available for AX Series products in the following documents. These documents are included on the documentation CD shipped with your AX Series product, and also are available on the A10 Networks support site:

- *AX Series Installation Guides*
- *AX Series LOM Reference*
- *AX Series System Configuration and Administration Guide*
- *AX Series IPv4-to-IPv6 Transition Solutions Guide*
- *AX Series Traffic Logging Guide for IPv6 Migration*
- *AX Series GUI Reference*
- *AX Series CLI Reference*
- *AX Series MIB Reference*

Make sure to use the basic deployment instructions in the *AX Series Installation Guide* for your AX model, and in the *AX Series System Configuration and Administration Guide*. Also make sure to set up your device's Lights Out Management (LOM) interface, if applicable.

Note: Some guides include GUI configuration examples. In these examples, some GUI pages may have new options that are not shown in the example screen images. In these cases, the new options are not applicable to the examples. For information about any option in the GUI, see the *AX Series GUI Reference* or the GUI online help.

Audience

This document is intended for use by network architects for determining applicability and planning implementation, and for system administrators for provision and maintenance of A10 Networks AX Series products.

Documentation Updates

Updates to these documents are published periodically to the A10 Networks support site, on an updated documentation CD (posted as a zip archive). To access the latest version, please log onto your A10 support account and navigate to the following page: Support > AX Series > Technical Library.

http://www.a10networks.com

A10 Virtual Application Delivery Community

You can use your A10 support login to access the A10 Virtual Application Delivery Community (VirtualADC). The VirtualADC is an interactive forum where you can find detailed information from product specialists. You also can ask questions and leave comments. To access the VirtualADC, navigate here:

http://www.a10networks.com/adc/

End User License Agreement 3

Obtaining Technical Assistance 7

Collecting System Information 7

About This Document 9

Audience 10

Documentation Updates 10

A10 Virtual Application Delivery Community 10

Using the CLI 33

System Access 33

Session Access Levels 33

High Availability Status in Command Prompt 34

IP Version Support 35

CLI Quick Reference 35

Context-Sensitive Help 36
The “no” Form of Commands 37
Command History 37
Editing Features and Shortcuts 38
Searching and Filtering CLI Output 42
Regular Expressions 42
Special Character Support in Strings 43

EXEC Commands 47

backup log 48
backup system 50
enable 51
exit 51
health-test 52
help 53
no 53
ping 53
show 55
ssh 55
telnet 56
traceroute 57

Privileged EXEC mode Commands 59

axdebug 59
backup log 59
backup system 59
clear 59
clock 63
configure 64
debug 64
diff 65
disable 66
exit 67
export 67
health-test 68
help 68
import 69
locale 70
no 71
ping 71
reboot 71
reload 73
repeat 74
show 75
shutdown 75
ssh 75
telnet 76
terminal 76
traceroute 77
write 77
write terminal 78

Config Commands: Global 79

6rd 79
access-list (standard) 80
access-list (extended) 82
accounting 87
admin 90
admin lockout 93
arp 94
arp timeout 94
audit 95
authentication 96
authorization 97
axdebug 99
backup periodically 99
banner 101
bfd echo 102
bfd enable 103

bfd interval 103
bgp extended-asn-cap 104
bgp nexthop-trigger 104
boot-block-fix 105
bootimage 105
bpdu-fwd-group 106
bridge-vlan-group 107
class-list (for many pools, standard NAT) 109
class-list (for IPv6 migration features) 110
clock timezone 110
convert-passwd 111
copy 112
debug 114
delete startup-config 114
disable 114
disable-management 115
do 117
ds-lite 118
enable 118
enable-core 119
enable-def-vlan-l2-forwarding 119
enable-jumbo 120
enable-management 121
enable-password 122
end 123
erase 123
exit 124
extended-stats 124
fixed-nat 124
floating-ip 125
glid 125
ha 125
health external 126
health global 127
health monitor 128
health postfile 129
hostname 130
icmp-rate-limit 131
interface 132
ip 132
ip-list 132
ipv6 133
key chain 133
l3-vlan-fwd-disable 134
lacp system-priority 135
lacp-trunk 135
link 137

locale 138
logging auditlog host 139
logging target severity-level 139
logging buffered 141
logging email buffer 141
logging email filter 142
logging email-address 144
logging export 145
logging facility 146
logging host 146
lsn-lid 147
lsn-rule-list 147
lw-4o6 147
mac-address 147
mac-age-time 148
maximum-paths 149
mirror-port 149
monitor 150
multi-config 151
nat46-stateless 152
nat64 152
netflow 152
no 155
ntp 156
ping 157
radius-server 157
raid 159
restore 159
route-map 160
router protocol 163
router log file 164
router log log-buffer 165
router log record-priority 165
router log stdout 165
router log trap 166
run-hw-diag 166
session strict-aging-on-clear 168
session-filter 168
sflow 170
slb 173
smtp 173
snmp-server community 174
snmp-server contact 175
snmp-server enable 175
snmp-server group 180
snmp-server host 181
snmp-server location 181

snmp-server user 182
snmp-server view 183
stats-data-disable 183
stats-data-enable 184
system {all-vlan-limit | per-vlan-limit} 185
system module-ctrl-cpu 186
system resource-usage 186
system template 189
system ve-mac-scheme 189
system-reset 190
tacacs-server 191
techreport 192
terminal 193
tftp blksize 194
trunk 195
tx-congestion-ctrl 197
update 198
upgrade 198
vlan 199
web-service 200
write 201
write terminal 202

Config Commands: Interface 203
access-list 203
bfd 204
bcast-rate-limit (management interface only) 205
cpu-process 206
disable 207
duplexity 208
enable 208
flow-control 209
icmp-rate-limit 209
interface 210
ip address 211
ip control-apps-use-mgmt-port (management interface only) 212
ip default-gateway (management interface only) 213
ip helper-address 214
ip nat 215
ip ospf 216
ip rip 216
{ip | ipv6} router isis 216
{ip | ipv6} stateful-firewall 217
ipv6 (on management interface) 217
ipv6 access-list 218
ipv6 address 218
ipv6 enable 219

ipv6 nat inside 219
ipv6 nat outside 220
ipv6 ndisc router-advertisement 220
ipv6 ospf 225
ipv6 rip split-horizon 225
ipv6 router isis 225
ipv6 router ospf 225
ipv6 router rip 225
isis 226
l3-vlan-fwd-disable 226
lacp port-priority 227
lacp timeout 227
lacp trunk 228
lacp udld-timeout 229
load-interval 229
lw-406 230
monitor 230
mtu 231
name 232
ospf 232
speed 233

Config Commands: VLAN 235

name 236
router-interface 236
tagged 237
untagged 238

Config Commands: IP 239

ip anomaly-drop 239
ip as-path 241
ip community-list 242
ip dns 243
ip extcommunity-list 243
ip frag max-reassembly-sessions 244
ip frag timeout 244
ip icmp disable 245
ip nat alg pptp 245
ip nat allow-static-host 245
ip nat icmp always-source-nat-errors 246
ip nat icmp respond-to-ping 246
ip nat inside 247
ip nat lsn 248
ip nat pcp 248
ip nat pool 248
ip nat pool-group 250

ip nat range-list 251
ip nat reset-idle-tcp-conn 252
ip nat template http-alg 252
ip nat template logging 253
ip nat template pcp 253
ip nat translation 253
ip prefix-list 254
ip prefix-list list-id description 257
ip prefix-list sequence-number 258
ip route 258
ip stateful-firewall 260

Config Commands: IPv6 265

ipv6 access-list 266
ipv6 frag timeout 269
ipv6 icmpv6 disable 269
ipv6 nat icmpv6 270
ipv6 nat inside 270
ipv6 nat pool 270
ipv6 neighbor 271
ipv6 ospf display 272
ipv6 pmtu {disable | enable} 273
ipv6 pmtu timeout 273
ipv6 prefix-list 273
ipv6 prefix-list list-id description 275
ipv6 prefix-list sequence-number 276
ipv6 route 276
ipv6 stateful firewall 277

Config Commands: Router – RIP 279

Enabling RIP....... 279
IPv4 RIP Configuration Commands 281
Global IPv4 RIP Commands 281
cisco-metric-behavior 281
default-information originate 281
default-metric 282
distance 282
distribute-list 283
maximum-prefix 284
neighbor 285
network 285
offset-list 286
passive-interface 287
recv-buffer-size 287
redistribute 288

route ... 291
timers ... 291
version ... 292
Interface-Level IPv4 RIP Commands ... 293
ip rip authentication ... 293
ip rip receive version ... 294
ip rip receive-packet ... 294
ip rip send version ... 294
ip rip send-packet ... 295
ip rip split-horizon ... 295
IPv6 RIP Configuration Commands ... 296
Global IPv6 RIP Commands ... 296
aggregate-address ... 296
cisco-metric-behavior ... 296
default-information originate ... 297
default-metric ... 297
distribute-list ... 297
neighbor ... 299
offset-list ... 300
passive-interface ... 301
recv-buffer-size ... 301
redistribute ... 302
route ... 305
route-map ... 305
timers ... 306
Interface-Level IPv6 RIP Command ... 307
ipv6 rip split-horizon ... 307
RIP Show Commands ... 308
show ip rip database ... 308
show ipv6 rip database ... 308
RIP Clear Commands ... 308
clear ip rip route ... 308
clear ipv6 rip route ... 309
Config Commands: Router – OSPF 311
Enabling OSPF ... 311
Global Configuration Commands Applicable to OSPFv2 or OSPFv3 ... 312
area area-id default-cost ... 312
area area-id range ... 313
area area-id stub ... 313
area area-id virtual-link ... 314
auto-cost reference bandwidth ... 315

bfd 316
default-metric 316
distribute-internal 317
ha-standby-extra-cost 318
log-adjacency-changes 319
max-concurrent-dd 319
maximum-area 319
passive-interface 320
redistribute 321
router-id 325
timers spf exp 326

Global Configuration Commands Applicable to OSPFv2 Only 327

area area-id authentication 327
area area-id filter-list 327
area area-id multi-area-adjacency 328
area area-id nssa 329
area area-id shortcut 330
capability opaque 330
compatible rfc1583 331
default-information originate 331
distance 332
distribute-list 333
host ipaddr area 334
neighbor 334
network 335
ospf abr-type 336
overflow database 337
summary-address 337

Global Configuration Commands Applicable to OSPFv3 Only 338

Interface-level Configuration Commands 338

ip ospf 338
ipv6 ospf cost 341
ipv6 ospf dead-interval 342
ipv6 ospf hello-interval 342
ipv6 ospf mtu-ignore 343
ipv6 ospf neighbor 343
ipv6 ospf network 344
ipv6 ospf priority 344
ipv6 ospf retransmit-interval 345
ipv6 ospf transmit-delay 345
ospf 346

OSPF Show Commands 348

show {ip | ipv6} ospf 348
show ip ospf border-routers 349

show ip ospf database 349
show ipv6 ospf database 351
show {ip | ipv6} ospf interface 353
show ip ospf multi-area-adjacencies 354
show {ip | ipv6} ospf neighbor 354
show ip ospf redistributed 355
show {ip | ipv6} ospf route 357
show ipv6 ospf topology 357
show {ip | ipv6} ospf virtual-links 358

Config Commands: Router – IS-IS 359

Enabling IS-IS 359

Global IS-IS Configuration Commands 360

address-family 360
adjacency-check 361
area-password 362
authentication 363
bfd 364
default-information originate 364
distance 365
domain-password 365
ha-standby-extra-cost 366
hostname dynamic 366
ignore-lsp-errors 367
is-type 367
log-adjacency-changes 367
lsp-gen-interval 368
lsp-refresh-interval 368
max-lsp-lifetime 368
metric-style 369
net 371
passive-interface 372
protocol-topology 373
redistribute 373
restart-timer 377
set-overload-bit 377
spf-interval-exp 378
summary-address 379

Interface-level IS-IS Configuration Commands 380

isis authentication 380
isis bfd 381
isis circuit-type 382
isis csnp-interval 382
isis hello padding 383
isis hello-interval 383

isis hello-multiplier 384
isis lsp-interval 384
isis mesh-group 385
isis metric 385
isis network 386
isis password 386
isis priority 387
isis restart-hello-interval 387
isis retransmit-interval 388
isis wide-metric 388

Show Commands for IS-IS 389

show ip isis [tag] route 389
show isis counter 390
show isis [tag] database 390
show isis interface 391
show isis [tag] topology 393
show ipv6 isis [tag] route 393
show ipv6 isis [tag] topology 394

Config Commands: Router – BGP 395

Enabling BGP 395

BGP Configuration Commands 396

Commands at the Global Configuration Level 396
bgp extended-asn-cap 396
bgp nexthop-trigger 397
Commands at the BGP Router Configuration Level 397
address-family 397
aggregate-address 400
auto-summary 400
bgp bestpath always-compare-med 400
bgp bestpath 401
bgp dampening 401
bgp default 402
bgp deterministic-med 403
bgp enforce-first-as 403
bgp fast-external-failover 404
bgp log-neighbor-changes 404
bgp nexthop-trigger-count 404
bgp router-id 405
bgp scan-time 405
distance 405
neighbor activate 407
neighbor advertisement-interval 407
neighbor allowas-in 408

neighbor as-origination-interval 408
neighbor capability 409
neighbor collide-established 410
neighbor connection-retry-time 411
neighbor default-originate 412
neighbor description 412
neighbor disallow-infinite-holdtime 413
neighbor distribute-list 413
neighbor dont-capability-negotiate 414
neighbor ebgp-multihop 414
neighbor enforce-multihop 415
neighbor fall-over 415
neighbor filter-list 416
neighbor maximum-prefix 417
neighbor next-hop-self 417
neighbor override-capability 418
neighbor passive 418
neighbor password 419
neighbor peer-group 419
neighbor prefix-list 420
neighbor remote-as 421
neighbor remove-private-AS 421
neighbor route-map 422
neighbor send-community 422
neighbor shutdown 423
neighbor soft-reconfiguration 424
neighbor strict-capability-match 424
neighbor timers 425
neighbor unsuppress-map 425
neighbor update-source 426
neighbor version 427
neighbor weight 427
network 428
redistribute 429
synchronization 431
timers 431

BGP Show Commands 432

show [ip] bgp ipv4addr 432
show [ip] bgp ipv6addr 432
show bgp ipv4 {multicast | unicast} 433
show bgp ipv4 neighbors 435
show bgp ipv4 prefix-list 436
show bgp ipv4 quote-regexp 436
show bgp ipv4 summary 436
show bgp ipv6 437
show bgp nexthop-tracking 440

show bgp nexthop-tree-details ... 440
show ip bgp attribute-info ... 440
show ip bgp cidr-only ... 440
show [ip] bgp community ... 440
show ip bgp community-info ... 441
show [ip] bgp community-list ... 441
show [ip] bgp dampening ... 442
show [ip] bgp filter-list ... 442
show [ip] bgp inconsistent-as ... 442
show ip bgp ipv4 ... 443
show [ip] bgp neighbors ... 445
show [ip] bgp paths ... 447
show [ip] bgp prefix-list ... 447
show [ip] bgp quote-regexp ... 447
show [ip] bgp regexp ... 447
show [ip] bgp route-map ... 447
show ip bgp scan ... 448
show [ip] bgp summary ... 448
show ip bgp view ... 448

BGP Clear Commands ... 449

clear [ip] bgp {* | AS-num} ... 449
clear [ip] bgp ipv4addr ... 450
clear [ip] bgp ipv6addr ... 451
clear ip bgp dampening ... 451
clear [ip] bgp external ... 451
clear ip bgp flap-statistics ... 452
clear [ip] bgp ipv4 ... 452
clear [ip] bgp ipv6 ... 453
clear [ip] bgp peer-group ... 453
clear [ip] bgp view ... 454

Config Commands: Large Scale NAT 455

LSN Configuration Commands ... 455

class-list (for LSN) ... 455
ip nat inside (for LSN) ... 457
ip nat lsn alg ... 457
ip nat lsn alg sip rtp-stun-timeout ... 458
ip nat lsn attempt-port-preservation ... 458
ip nat lsn endpoint-independent-filtering ... 459
ip nat lsn endpoint-independent-mapping ... 460
ip nat lsn full-cone ... 461
ip nat lsn hairpinning ... 462
ip nat lsn icmp ... 463
ip nat lsn ip-selection ... 464
ip nat lsn logging default-template ... 465

ip nat lsn logging pool 466
ip nat lsn port-batching 466
ip nat lsn port-overloading allow-different-user 467
ip nat lsn port-overloading enable 467
ip nat lsn port-overloading unique 468
ip nat lsn port-reservation 468
ip nat lsn radius server 469
ip nat lsn stun-timeout 471
ip nat lsn syn-timeout 472
ip nat lsn tcp mss-clamp 472
ip nat lsn tcp reset-on-error 473
ip nat pool (for LSN) 473
ip nat pool-group 476
ip nat template http-alg 477
ip nat template logging 479
lsn-lid 479
lsn-rule-list 482

LSN Show Commands........485

show ip nat lsn alg 485
show ip nat lsn full-cone-sessions 489
show ip nat lsn inside-user 491
show ip nat lsn pool-statistics 493
show ip nat lsn port-overloading config 495
show ip nat lsn port-reservations 495
show ip nat lsn radius server 496
show ip nat lsn radius table 496
show ip nat lsn statistics 497
show ip nat lsn system-status 501
show ip nat lsn user-quota-sessions 502
show lsn-lid 504
show lsn-rule-list 504

Config Commands: Port Control Protocol 505

PCP Configuration Commands........506

ip nat pcp default-template 506
ip nat template pcp 506

PCP Show Commands........508

show ip nat pcp statistics 508

Config Commands: NAT64 / DNS64 513

DNS64 Configuration Commands........513

ip nat pool (for DNS64) 513
ip nat pool-group (for DNS64) 515
ipv6 nat pool (for DNS64) 517

nat64 prefix 518
slb server 518
slb service-group 520
slb template dns 521
slb virtual-server 525

NAT64 Configuration Commands 526

class-list (for NAT64) 526
ip nat outside 527
ipv6 nat inside 528
ip nat pool (for NAT64) 528
ip nat pool-group (for NAT64) 529
glid (for NAT64 override) 529
lsn-lid 530
nat64 alg 531
nat64 fragmentation df-bit-transparency 532
nat64 fragmentation inbound 533
nat64 fragmentation outbound 533
nat64 icmp 534
nat64 inside 535
nat64 prefix 535
nat64 tcp mss-clamp 535
nat64 tcp reset-on-error 536
nat64 user-quota-prefix-length 536
slb template policy 537

DNS64 / NAT64 Show Commands 539

show dns64 statistics 539
show nat64 alg 540
show nat64 conversion 541
show nat64 full-cone-sessions 541
show nat64 inside-user 542
show nat64 prefixes 545
show nat64 statistics 545
show nat64 user-quota-sessions 548

Config Commands: DS-Lite 551

DS-Lite Configuration Commands 551

class-list (for DS-Lite) 551
ds-lite alg 552
ds-lite fragmentation inbound 553
ds-lite fragmentation outbound 554
ds-lite icmp 555
ds-lite inside source 556
ip-checksum-error 556
l4-checksum-error 557

ds-lite port-reservation 557
ds-lite tcp mss-clamp 558
ds-lite tcp reset-on-error 559
DS-Lite Show Commands....559
show ds-lite alg 559
show ds-lite full-cone-sessions 560
show ds-lite inside-user 561
show ds-lite port-reservations 563
show ds-lite statistics 564
show ds-lite user-quota-sessions 567
Config Commands: Lightweight 4over6 569
Lightweight 4over6 Configuration Commands 570
lw-4o6 binding-table 570
lw-4o6 ha-group-id 571
lw-4o6 hairpinning 571
lw-4o6 icmp-inbound 572
lw-4o6 no-forward-match 573
lw-4o6 no-reverse-match 573
lw-4o6 use-binding-table 574
Lightweight 4over6 Show Commands 574
show lw-4o6 binding-table 574
show lw-4o6 statistics 575
Config Commands: Stateless NAT46 577
Stateless NAT46 Configuration Commands 578
nat46-stateless fragmentation inbound 578
nat46-stateless fragmentation outbound 578
nat46-stateless fragmentation outbound df-set 579
nat46-stateless prefix 579
nat46-stateless static-dest-mapping 580
Stateless NAT46 Show Commands 581
show nat46-stateless statistics 581
Config Commands: 6rd 585
6rd Configuration Commands....585
6rd domain 585
6rd fragmentation inbound 587
6rd fragmentation outbound 588
6rd fragmentation outbound df-set 589

6rd Show Commands..589

show 6rd statistics 589

Config Commands: Logging Template 593

ip nat template logging 593
slb server 601
slb service-group 603

Show Commands..605

show ip nat logging keywords 605
show ip nat logging statistics 606
show ip nat logging tcp-svr-status 606
show ip nat template logging 607
show slb server 607
show slb service-group 608

Config Commands: Fixed-NAT 609

Fixed-NAT Configuration Command..609

fixed-nat 609

Fixed-NAT Show Commands..611

show fixed-nat alg 611
show fixed-nat full-cone-sessions 612
show fixed-nat inside-user 612
show fixed-nat nat-address 613
show fixed-nat statistics 613

Config Commands: Server Resource Commands 617

slb buff-thresh 617
slb fast-path-disable 618
slb gateway-health-check 618
slb l2l3-trunk-lb-disable 619
slb msl-time 620
slb server 620
slb service-group 621
slb ssl-module 621
slb template dns 621
slb template policy 624
slb template port 627
slb template server 633
slb template virtual-port 637
slb template virtual-server 640
slb virtual-server 643

Config Commands: Virtual Servers 645

arp-disable 645
disable 646
enable 646
extended-stats 647
ha-dynamic 647
ha-group 647
port 648
redistribution-flagged 648
stats-data-disable 649
stats-data-enable 649
template logging 649
template policy 649
template virtual-server 650

Config Commands: Virtual Server Ports 651

access-list 651
conn-limit 653
def-selection-if-pref-failed 654
disable 655
enable 655
extended-stats 656
name 656
no-dest-nat 656
service-group 657
snat-on-vip 658
source-nat 658
stats-data-disable 659
stats-data-enable 659
template 660
template virtual-port 661
use-default-if-no-server 661
use-rcv-hop-for-resp 662

Config Commands: Health Monitors 663

disable-after-down 663
method 664
override-ipv4 667
override-ipv6 667
override-port 667
strictly-retry-on-server-error-response 668

Config Commands: High Availability 669

ha arp-retry ... 669
ha check gateway ... 670
ha check route ... 671
ha check vlan ... 673
ha conn-mirror ... 674
ha force-self-standby ... 675
ha forward-l4-packet-on-standby ... 675
ha group ... 675
ha id ... 676
ha interface ... 677
ha l3-inline-mode ... 678
ha link-event-delay ... 679
ha ospf-inline vlan ... 680
ha preemption-enable ... 680
ha restart-port-list ... 681
ha restart-time ... 682
ha start-redundant-msg-count ... 682
ha stop-redundant-msg-count ... 683
ha sync ... 684
ha time-interval ... 687
ha timeout-retry-count ... 687

Show Commands 689

show 6rd ... 689
show access-list ... 689
show admin ... 690
show arp ... 693
show audit ... 694
show axdebug file ... 694
show axdebug filter ... 695
show axdebug status ... 695
show backup ... 695
show bfd ... 695
show bgp ... 698
show bootimage ... 699
show bpdu-fwd-group ... 699
show bridge-vlan-group ... 700
show class-list ... 700
show clns ... 701
show clock ... 701
show core ... 702
show cpu ... 702
show debug ... 703
show disk ... 704
show dns ... 705
show dns cache ... 706

show dns64 707
show ds-lite 708
show dumpthread 708
show environment 708
show errors 709
show fixed-nat 714
show glid 714
show ha 715
show ha mac 718
show hardware 718
show health 719
show history 723
show icmp 724
show interfaces 725
show interfaces statistics 726
show ip 727
show ip bgp 727
show ip dns 727
show {ip | ipv6} fib 727
show {ip | ipv6} fragmentation statistics 728
show ip helper-address 731
show {ip | ipv6} interfaces 735
show {ip | ipv6} isis 736
show ip nat 736
show ipv6 nat interfaces 740
show ipv6 ndisc 740
show ipv6 neighbor 742
show {ip | ipv6} ospf 742
show {ip | ipv6} protocols 742
show {ip | ipv6} rip 743
show ip route 743
show ip-list 744
show ipmi 744
show ipv6 route 744
show ipv6 traffic 745
show isis 745
show key-chain 745
show lacp 746
show locale 747
show log 747
show lsn-lid 748
show lsn-rule-list 748
show lw-4o6 749
show mac-address-table 751
show management 752
show memory 752
show mirror 753

show monitor 753
show nat46-stateless 754
show nat64 754
show netflow 754
show ntp 755
show process 756
show radius-server 756
show reboot 757
show router log file 757
show running-config 758
show session 760
show sflow 765
show shutdown 766
show slb l4 766
show slb performance 770
show slb server 771
show slb service-group 772
show slb switch 772
show slb template 777
show slb virtual-server 777
show smtp 778
show startup-config 778
show statistics 780
show system platform 781
show system resource-usage 782
show tacacs-server 783
show techsupport 783
show terminal 784
show tftp 784
show trunk 785
show version 786
show vlans 787
show web-service 787
AX Debug Commands 789
capture 790
count 793
delete 793
filter 794
incoming | outgoing 796
length 796
maxfile 797
outgoing 797
timeout 797

show health stat Up / Down Causes 799

Up Causes....................799

Down Causes....................800

Using the CLI

This chapter describes how to use the Command Line Interface (CLI) for the AX Series™ Advanced Traffic Manager from A10 Networks. The commands and their options are described in the other chapters.

System Access

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 AX CLI is generally 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.

Session Access Levels

As a security feature, the AX Series 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 AX Series commands (configuration mode, configuration submodes and management mode) and can be password protected to allow only authorized users the ability to configure or maintain the system.

User EXEC Level: AX>

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

For example, when an EXEC session is started, the AX Series will display the AX> prompt. 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 AX device. To list the commands available at the User EXEC level, type a question mark (**?**) then press Enter at the prompt; for example, AX>**?**.

Privileged EXEC Level: AX#

This level is also called the “enable” level because the **enable** command is used to gain access. Privileged EXEX 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 AX> prompt. If an enable password is configured, the AX Series will then prompt for that password. When the correct enable password is entered, the AX Series prompt will change from AX> to AX# indicating that the user is now at the “Privileged EXEC” level. To switch back to the “User EXEC” level, type **disable** at the AX# 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: AX(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:

```
AX>enable
```

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

```
AX#config
```

The prompt changes to include “(config)”:

```
AX(config)#
```

High Availability Status in Command Prompt

If High Availability (HA) is configured on the AX device, the command prompt shows the HA status, which can be one of the following:

- AX-Active#
- AX-Standby#
- AX-Forced_Standby#

Note: If HA is not configured, the prompt is simply the hostname (“AX” by default).

Display of the HA status is configurable. (See “terminal” on page 193.)

IP Version Support

Unless otherwise noted, where “*ipaddr*” is shown as a command option, an IPv4 or IPv6 address can be specified.

CLI Quick Reference

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

```
AX>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.

AX>
```

Context-Sensitive Help

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 following commands:

Prompt	Command	Purpose
AX> or AX# or (config)#	**Help**	Displays the CLI Quick Reference
	abbreviated-command-help?	Lists all commands beginning with abbreviation before the (**?**). If the abbreviation is not found, the AX Series returns: % Ambiguous command
	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 a 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. AX#**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. AX# **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 the AX Series 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.

```
AX#co?
config          Entering config mode
```

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

```
AX#config ?
terminal        Config from the terminal
<cr>
```

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 **config** command is **config terminal** (configure manually from the terminal connection).

The “no” Form of Commands

Most configuration commands have a **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.

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
- Recalling commands
- Disabling the command history feature

Setting the Command History Buffer Size

The AX Series records ten 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 following command in EXEC mode:

Convention	Description
AX# **terminal history** [**size** *number-of-lines*]	Enables the command history feature for the current terminal session.
AX# **no terminal history size**	Resets the number of commands saved in the history buffer to the default of 256 commands.
AX(config)# **terminal history** [**size** *number-of-lines*]	Enables the command history feature for the all the configuration sessions.

Recalling Commands

To recall commands from the history buffer, use one of the following commands or key combinations:

Command or Key Combination	Description
Ctrl+P or **Up Arrow** key.[1]	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl+N or **Down Arrow** key. [1]	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.
AX> **show history**	While in EXEC mode, lists the most recent commands entered.

[1] The arrow keys function only on ANSI-compatible terminals.

Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the AX Series CLI. The following subsections describe these features:

- Moving the cursor on the command line
- Completing a partial command name
- Recalling deleted entries
- Editing command lines that wrap
- Deleting entries

- Continuing output at the --MORE-- prompt
- Re-displaying the current command line

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 the following table, characters bolded in the Function Summary column indicate the relation between the letter used and the function.

Keystrokes	Function Summary	Function Details
`Left Arrow` `or` **`ctrl+B`**	**B**ack 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`**	**F**orward 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`	**E**nd 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:

```
AX# conf<tab>
AX# config
```

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:

```
AX#te
% Ambiguous command

AX#
```

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:

```
AX#te?
  telnet    Open a tunnel connection
  terminal  Set terminal line parameters
AX#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, you can use the following keys or key combinations to delete command 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 AX Series 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 to recall and modify previous complex command entries. See the `Recalling Commands` section in this chapter for information about recalling previous 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.

Redisplay 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 of the following key combinations:

Keystrokes	Purpose
`ctrl+L` or **`ctrl+R`**	Re-displays the current command line

Searching and Filtering CLI Output

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 following output filtering options:

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

Use “ **|** ” as a delimiter between the **show** command and the display filter.

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

```
AX(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 in this example 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”. (See “Regular Expressions” on page 42.)

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

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

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 **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. The following table lists the keyboard characters that have special meaning.

Character	Meaning
.	Matches any single character, including white space
*	Matchers 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 a space.

Special Character Support 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.

Special Character Support in Password Strings

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

For information about the supported password length, see the CLI help or the command entry in this document.

Admin and Enable Passwords

Admin and enable passwords can contain any ASCII characters in the following ranges: 0x20-0x7e and 0x80-0xFF.

RADIUS Shared Secrets

Same as admin and enable passwords.

SNMPv3 user authentication passwords

Same as admin and enable passwords.

Passwords used for file import / export

All of the characters in the following range are supported: 0x20-0x7E.

Passwords used for server access in health monitors

Most of the characters in the following range are supported: 0x20-0x7E. However, the following characters are not supported in the current release:

```
'  " <  >  &  \  /  ?
```

SSL certificate passwords

Most of the characters in the following ranges are supported: 0x20-0x7E and 0x80-0xFF. However, the following characters are not supported in the current release:

```
'  " <  >  &  \  /  ?
```

SMTP passwords

Same as SSL certificate passwords.

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 take 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.)

`Note:` 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.

EXEC Commands

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:

```
AX>
```

backup log

Description

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

Syntax

```
[no] backup log period {all | day | month | week}

[no] backup log expedite

backup log [use-mgmt-port] url

backup log stats-data [use-mgmt-port] url
```

Parameter	Description
`expedite`	Allocates additional CPU to the backup process. This option allows up to 80% CPU utilization to be devoted to the log backup process.
`period {all | day | month | week}`	Specifies the period to back up: **all** – Backs up all log messages contained in the log buffer. **day** – Backs up the log messages generated during the most recent 24 hours. **month** – Backs up the log messages generated during the most recent 30 days. **week** – Backs up the log messages generated during the most recent 7 days.
`[use-mgmt-port]` *`url`*	Saves a backup of the log to a remote server. The **use-mgmt-port** option 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 AX device attempts to use the data route table to reach the remote device through a data interface. The *url* specifies the file transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted

	for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp**://*host*/*file* **ftp**://[*user*@]*host*[:*port*]/*file* **scp**://[*user*@]*host*/*file* **rcp**://[*user*@]*host*/*file*
stats-data [use-mgmt-port] *url*	Backs up statistical data from the GUI. The **use-mgmt-port** and *url* options are the same as described above.

Default The configurable backup options have the following default values:

- **expedite** – The AX device allows up to 50% CPU utilization for log backup.
- **period** – month

Mode Privileged EXEC or global configuration

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.

Example The following commands change the backup period to **all**, allow up to 80% CPU utilization for the backup process, and back up the log:

```
AX>backup log period all
AX>backup log expedite
AX>backup log scp://192.168.20.161:/log.tgz
...
```

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

```
AX>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

Back up the system.

Syntax Description

```
backup system [use-mgmt-port] url
```

Parameter	Description
`system`	Backs up the startup-config file and SSL certificates and keys into a tar file.
`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 AX device attempts to use the data route table to reach the remote device through a data interface.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp:**//*host*/*file* **ftp:**//[*user*@]*host*[:*port*]/*file* **scp:**//[*user*@]*host*/*file* **rcp:**//[*user*@]*host*/*file*

Default N/A

Mode Privileged EXEC or global configuration

Example The following command backs up the system:

```
AX>backup system tftp://1.1.1.1/back_file
```

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 #.

```
AX>enable
Password: <letmein>
AX# disable
AX>
```

exit

Description

Close an active terminal session by logging off the system.

Syntax

```
exit
```

Mode

EXEC and Privileged EXEC

Usage

Use the `exit` command in EXEC mode to exit the active session (log off the device).

Example

In the following example, the `exit` (global) command is used to move from global configuration mode to privileged EXEC mode, the `disable` command is used to move from privileged EXEC mode to user EXEC mode, and the **exit** (EXEC) command is used to log off (exit the active session):

```
AX(config)#exit
AX#disable
AX>exit
```

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** *portnum*]

Parameter	Description
ipaddr | **ipv6** *ipv6addr*	Specifies the IPv4 or IPv6 address of the device to test.
count *num*	Specifies the number of health checks to send to the device. You can specify 1-65535.
monitorname *monitor-name*	Specifies the health monitor to use. The health monitor must already be configured.
port *portnum*	Specifies the protocol port to test, 1-65535.

Default

Only the IP address is required. The other parameters have the following defaults:

- **count** – 1
- **monitorname** – ICMP ping, the default Layer 3 health check
- **port** – Override port number set in the health monitor configuration, if one is set. Otherwise, this option is not set by default.

Mode

EXEC, Privileged EXEC, and global config

Usage

If an override IP address and protocol port are set in the health monitor configuration, the AX 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:

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

help

Description

Display a description of the interactive help system of the AX Series.

Syntax

```
help
```

Example

(See “CLI Quick Reference” on page 35.)

no

Description

See “no” on page 71. This command is not used at this level.

ping

Description

Send an ICMP echo packet to test network connectivity.

Syntax

```
ping [ipv6] {hostname | ipaddr}
[data HEX-word]
[flood]
[interface {ethernet port-num | ve ve-num |
  management}]
[repeat count]
[size num]
[timeout secs]
[ttl num]
[source {ipaddr | ethernet port-num | ve ve-num}]
```

Parameter	Description
`[ipv6]` *hostname* | *ipaddr*	Target of the ping.
data *HEX-word*	Hexadecimal data pattern to send in the ping. The pattern can be 1-8 hexadecimal characters long.
flood	Sends a continuous stream of ping packets, by sending a new packet as soon as a reply to the previous packet is received.

interface {**ethernet** *port-num* | **ve** *ve-num* | **management**}	Uses the specified interface as the source address of the ping.
repeat *count*	Number of times to send the ping, 1-10000000 (ten million).
size *num*	Size of the datagram, 1-10000.
timeout *secs*	Number of seconds the AX device waits for a reply to a sent ping packet, 1-2100 seconds.
ttl *num*	Maximum number of hops the ping is allowed to traverse, 1-255.
source *ipaddr* | **ethernet** *port-num* | **ve** *ve-num*	Forces the AX device to give the specified IP address, or the IP address configured on the specified interface, as the source address of the ping.

Default

This command has the following defaults:

- **data** – not set
- **flood** – disabled
- **interface** – not set. The AX 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.)
- **repeat** – 5
- **size** – datagram size is 84 bytes
- **timeout** – 10 seconds
- **ttl** – 1
- **source** – not set. The AX device looks up the route to the ping target and uses the interface associated with the route.

Mode

EXEC and Privileged EXEC

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 of each ping packet is 1 second.

To terminate a ping session, type ctrl+c.

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

```
AX>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 AX Ethernet port 1. The ping has data pattern “ffff”, is 1024 bytes long, and is sent 100 times.

```
AX#ping data ffff repeat 100 size 1024 source ethernet 1 10.10.1.20
```

show

Description Show system or configuration information.

Syntax

```
show options
```

Default N/A

Mode EXEC and Privileged EXEC

Usage For information about the **show** commands, see “Show Commands” on page 689.

ssh

Description Establish a Secure Shell (SSH) connection from the AX Series to another device.

Syntax

```
ssh [use-mgmt-port] {host-name | 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 AX device attempts to use

	the data route table to reach the remote device through a data interface.
host-name	Host name of a remote system.
ipaddr	The IP address of a remote system.
login-name	User name to log into the remote system.
protocol-port	TCP port number on which the remote system listens for SSH client traffic.

Default By default, the AX device will use a data interface as the source interface. The management interface is not used unless you specify the **use-mgmt-port** option. The default *protocol-port* is 22.

Mode EXEC and Privileged EXEC

Usage SSH version 2 is supported. SSH version 1 is not supported.

telnet

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

Syntax

```
telnet [use-mgmt-port] {host-name | 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 AX device attempts to use the data route table to reach the remote device through a data interface.
host-name	Host name of a remote system.
ipaddr	The IP address of a remote system.
protocol-port	TCP port number on which the remote system listens for Telnet traffic.

Default By default, the AX device will use a data interface as the source interface. The management interface is not used unless you specify the **use-mgmt-port** option. The default *protocol-port* is 23.

Mode EXEC and Privileged EXEC

Example

The following command opens a Telnet session from the AX to another AX at IP address 10.10.4.55:

```
AX>telnet 10.10.4.55
Trying 10.10.4.55...
Connected to 10.10.4.55.
Escape character is '^]'.
Welcome to AX3200
AX login:
```

traceroute

Description

Display the router hops through which a packet sent from the AX Series device can reach a remote device.

Syntax

```
traceroute [ipv6] [use-mgmt-port]
{host-name | ipaddr)
```

Parameter	Description
ipv6	Indicates that the target address is an IPv6 address.
use-mgmt-port	Uses the management interface as the source interface. The management route table is used to reach the device. By default, the AX device attempts to use the data route table to reach the remote device through a data interface.
{hostname | ipaddr)	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:

```
AX#traceroute 192.168.10.99
traceroute to 192.168.10.99 (192.168.10.99), 30 hops max, 40 byte pack-
ets
 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
 ...
```

Privileged EXEC mode Commands

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:

```
AX#
```

axdebug

Description Enters the AX debug subsystem. (See “AX Debug Commands” on page 789.)

backup log

Description Configure log backup options and save a backup of the system log. (See “backup log” on page 48.)

backup system

Back up the system. (See “backup system” on page 50.)

clear

Description Clear statistics or reset functions. Sub-command parameters are required for specific sub-commands.

Syntax **`clear`** *`sub-command parameter`*

Sub-Command	Description
`6rd`	Clears IPv6 Rapid Deployment (6rd) statistics.
`access-list` `{`*`acl-num`* `|` **`all`**`}`	Clears ACL statistics.

admin session {*session-id* | **all**}	Clears admin sessions.
arp {*options*}	Clears ARP entries.
bfd statistics	Clears Bidirectional Forwarding Detection (BFD) statistics.
bgp {*options*}	Clears information and statistics for Border Gate way Protocol (BGP). See “BGP Clear Commands” on page 655.
clns neighbors	Clears Connectionless-mode Network Service (CLNS) neighbor routes.
console	Kills the current login process and starts a new one.
core	Clears system core dump files.
dns {*options*}	Clears DNS cache entries or statistics.
dns64 statistics	Clears DNS64 statistics.
ds-lite statistics	Clears Dual-stack Lite (DS-Lite) statistics.
dumpthread	Clears dumpthread files.
fixed-nat *options*	Clears Fixed-NAT sessions or statistics.
ha	Clears High-Availability (HA) statistics.
health [**gateway**]	Clears health monitoring statistics.
icmp	Clears ICMP statistics.
ip bgp {*options*}	Clears information and statistics for Border Gate way Protocol (BGP). See “BGP Clear Commands” on page 449.
ip fragmentation statistics	Clears IP fragmentation statistics.
ip helper-address statistics	Clears IPv4 DHCP helper statistics.
ip nat {*options*}	Clears IPv4 NAT information or statistics.

ip ospf [*process-id*] **process**	Terminates OSPFv2 processing. The *process-id* option specifies the OSPFv2 process. If you omit this option, processing is terminated for all running OSPFv2 processes.
ip rip route {*options*}	Clears IPv4 Routing Information Protocol (RIP) routes.
ip route kernel	Clears stale IPv4 kernel routes.
ip stateful-firewall *options*	Clears IP stateful-firewall information or statistics.
ipv6 access-list {**all** | *acl-id*}	Clears IPv6 ACL statistics.
ipv6 fragmentation statistics	Clears IPv6 fragmentation statistics.
ipv6 nat pool statistics [*pool-name*]	Clears IPv6 NAT statistics.
ipv6 neighbor	Clears the IPv6 neighbor cache.
ipv6 ospf [*tag*] **process**	Terminates OSPFv3 processing. The *tag* option specifies the OSPFv3 instance (tag). If you omit this option, processing is terminated for all running OSPFv3 instances.
ipv6 rip route {*options*}	Clears IPv6 Routing Information Protocol (RIP) routes.
ipv6 route kernel	Clears stale IPv6 kernel routes.
ipv6 stateful-firewall *options*	Clears IPv6 stateful-firewall information or statistics.
ipv6 traffic	Clears IPv6 traffic statistics.
isis database	Clears the database for Intermediate System to Intermediate System (IS-IS).

lacp *{options}* Clears LACP information or statistics.

logging Clears the system log buffer.

lsn-rule-list *{options}* Clears statistics for LSN rule lists.

lw-4o6 *options* Clears information or statistics for Lightweight 4over6.

mac-address *{options}* Clears the MAC address table.

nat46-stateless statistics Clears statistics for stateless NAT46.

nat64 statistics Clears statistics for NAT64.

netflow statistics [**monitor** *monitor-name*] Clears NetFlow statistics.

router log file [*type*] Clears router log files. The *type* can be one of the following:

- **bgpd** [*file-num*] – Clears the specified BGP log file, or all BGP log files.
- **isisd** [*file-num*] – Clears the specified IS-IS log file, or all IS-IS log files.
- **nsm** [*file-num*] – Clears the specified Network Services Module (NSM) log file, or all NSM log files.
- **ospf6d** [*file-num*] – Clears the specified IPv6 OSPFv3 log file, or all OSPFv3 log files.
- **ospfd** [*file-num*] – Clears the specified IPv4 OSPFv2 log file, or all OSPFv2 log files.
- **ripd** [*file-num*] – Clears the specified IPv4 RIP log file, or all IPv4 RIP log files.
- **ripng** [*file-num*] – Clears the specified IPv6 RIP log file, or all IPv6 RIP log files.

If you do not specify a type, router logs of all types above are cleared.

sessions [*options*]	Clears sessions.
sflow statistics	Clears sFlow statistics.
slb {*options*}	Clears SLB statistics.
statistics [**interface ethernet** *portnum*]	Clears physical Ethernet interface statistics.

Default

N/A

Mode

Privileged EXEC mode or global configuration mode

Usage

To list the options available for a **clear** command, enter **?** after the command name. For example, to display the **clear arp** options, enter the following command: **clear arp ?**

On some AX models, entering either the **clear slb switch** or **clear slb l4** command clears all anomaly counters for both **show slb switch** *and* **show slb l4**. This applies to the following models: AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200.

Note on Clearing Sessions

After entering the **clear session** command, the AX 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 clears the counters on Ethernet interface 3:

```
AX#clear statistics interface ethernet 3
```

clock

Description

Set the system time and date.

Syntax

clock set *time day month year*

Parameter	Description
time	Format hh:mm:ss (24 hr.)
day	Format 1-31 – day of month
month	Format January, February, and so on.
year	Format 2007, 2008, and so on.

Note: The default time zone is GMT.

Mode Privileged EXEC mode

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

If you use the GUI or CLI to change the AX 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. For example, in the GUI, the graphs displayed on the Monitor > Overview page are cleared.

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, 2007.

```
AX#clock set 17:51:00 22 February 2007
```

configure

Description Enter the configuration mode from the Privileged EXEC mode.

Syntax `configure [terminal]`

Mode Privileged EXEC mode

Example Enter configuration mode.

```
AX#configure
AX(config)#
```

debug

Note: It is recommended to use the AXdebug subsystem instead of these **debug** commands. See “AX Debug Commands” on page 789.

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 **diff startup-config running-config** command compares the configuration profile that is currently linked to “startup-config” with the running-config. Similarly, the **diff startup-config** *profile-name* command compares the configuration profile that is currently linked to “startup-config” with the specified configuration profile.

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.

Example

The following command compares the configuration profile currently linked to “startup-config” with configuration profile “testcfg1”. This example is abbreviated for clarity. The differences between the profiles are shown in this example in bold type.

```
AX#diff startup-config testcfg1
!Current configuration: 13378 bytes                           (
!Configuration last updated at 19:18:57 PST Wed Jan 23 2008   (
!Configuration last saved at 19:19:37 PST Wed Jan 23 2008     (
!version 1.2.1                                                (
!                                                             (
hostname AX                                                   (
!                                                             (
clock timezone America/Tijuana                                (
!                                                             (
ntp server 10.1.11.100                                        (
!                                                             (
...
!                                                             (
interface ve 30                                               (
 ip address 30.30.31.1 255.255.255.0                          |  ip address
10.10.20.1 255.255.255.0
 ipv6 address 2001:144:121:3::5/64                            |  ipv6 address
fc00:300::5/64
!                                                             (
!                                                             (
                                                              > ip nat range-
list v6-1 fc00:300::300/64 2001:144:121:1::900/6
!                                                             (
ipv6 nat pool p1 2001:144:121:3::996 2001:144:121:3::999 netm <
!                                                             <
--MORE--
```

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.

```
AX#disable
AX>
```

Note: The prompt changes from # to >, indicating 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:

```
AX#exit
AX>
```

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

export

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

Syntax

```
export {class-list | ssl-cert | ssl-key |
ssl-crl | axdebug | debug_monitor}
file-name
[use-mgmt-port]
url
```

Parameter	Description
class-list	Exports an IP class list.
ssl-cert	Exports a certificate.
ssl-key	Exports a certificate key.
ssl-crl	Exports a Certificate Revocation List (CRL).
axdebug	Exports an AX debug capture file.
debug_monitor	Exports a debug monitor file.
file-name	Name of the file to export.
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 AX device attempts to use the data route table to reach the remote device through a data interface.

url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp:**//*host*/*file* **ftp:**//[*user*@]*host*[:*port*]/*file* **scp:**//[*user*@]*host*/*file* **rcp:**//[*user*@]*host*/*file*

Mode

Privileged EXEC mode or global configuration mode

Usage

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 directory path and file name is too long, Windows will not recognize the file. This limitation is not present on machines running Linux/Unix.

health-test

Description

See “health-test” on page 52.

help

Description

Display a description of the interactive help system of the AX Series.

Syntax

```
help
```

Example

(See “CLI Quick Reference” on page 35.)

import

Description Get a file from a remote site.

Syntax

```
import
{class-list | ssl-cert | ssl-key | ssl-crl }
file-name url
[period seconds]
```

Parameter	Description
class-list	Imports an IP class list.
feature-license	Imports a feature license.
license	Imports a license.
ssl-cert	Imports a certificate.
ssl-key	Imports a certificate key.
ssl-crl	Imports a Certificate Revocation List (CRL).
file-name	Specifies the filename to use on the target server.
url	Specifies the file transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp://***host***/***file* **ftp://**[*user*@]*host*[:*port*]**/***file* **scp://**[*user*@]*host***/***file* **rcp://**[*user*@]*host***/***file*
period *seconds*	Enables automated updates of the file. You can specify 60-31536000 seconds. (See “Usage” below.)

Mode Privileged EXEC mode or global configuration mode

Usage For SSL certificates and keys, this command is equivalent to the **slb ssl-load** command. You can use either one to import SSL certificates and keys.

Note: The AX device only supports certificates that are in Privacy-Enhanced Mail (PEM) format. The maximum supported certificate size is 16KB. To convert a certificate from Windows format to PEM format, see the “Importing SSL Certificates” chapter in the *AX Series System Configuration and Administration Guide*.

Periodic Updates

The **period** option simplifies update of imported files, especially files that are used by multiple AX devices. You can edit a single instance of the file, on the remote server, then configure each of AX device to automatically update the file to import the latest changes.

When you use this option, the AX 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.

locale

Description

Set the locale for the current terminal session.

Syntax

```
locale parameter
```

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

ja_JP.UTF-8	Japanese locale for Japan, encoding with UTF-8
ja_JP.EUC-JP	Japanese locale for Japan, encoding with EUC-JP

Default en_US.UTF-8

Mode Privileged EXEC mode or global configuration mode

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:

```
AX#no terminal history
AX#
```

ping

Test network connectivity. For syntax information, see “ping” on page 53.

reboot

Reboot the AX Series device.

Syntax

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

Parameter	Description
text	Reason for the reboot, 1-255 characters long.
in [*hh:*]*mm*	Schedule a reboot to take effect in the specified minutes or hours and minutes. The reboot must take place within approximately 24 hours.
at *hh:mm*	Schedule a reboot to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reboot is scheduled to take

	place at the specified time and date. If you do not specify the month and day, the reboot takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reboot for midnight.
month	Name of the month, any number of characters in a unique string.
day	Number of the day, 1-31.
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 AX Series (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the AX Series. To schedule reboots across several AX Series to occur simultaneously, the time on each AX Series must be synchronized with NTP. To display information about a scheduled reboot, use the **show reboot** command.

Example The following example immediately reboots the AX Series device:

```
AX(config)# reboot
System configuration has been modified. Save? [yes/no]:yes
Rebooting System Now !!!
Proceed with reboot? [yes/no]:yes
```

The following example reboots the AX Series device in 10 minutes:

```
AX(config)# reboot in 10
AX(config)# Reboot scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reboot? [yes/no]yes
AX(config)#
```

The following example reboots the AX Series device at 1:00 p.m. today:

```
AX(config)# reboot at 13:00
AX(config)# Reboot scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2
minutes)
Proceed with reboot? [yes/no]yes
AX(config)#
```

The following example reboots the AX Series device on Apr 20 at 4:20 p.m.:

```
AX(config)# reboot at 16:20 apr 20
AX(config)# Reboot scheduled for 16:20:00 PDT Sun Apr 20 2008 (in 38 hours and
9 minutes)
Proceed with reboot? [yes/no]yes
AX(config)#
```

The following example cancels a pending reboot:

```
AX(config)# reboot cancel
%Reboot cancelled.

***
*** --- REBOOT ABORTED ---
***
```

reload

Description

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

Syntax

```
reload
```

Mode

Privileged EXEC mode

Usage

The **reload** command restarts AX system processes and reloads the startup-config, without reloading the system image. To also reload the system image, use the **reboot** command instead. (See “reboot” on page 71.)

The AX device closes all sessions as part of the reload.

Example

The following command reloads an AX device:

```
AX(config)#reload
Reload AX ....Done.
AX(config)#
```

repeat

Description

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

Syntax

```
repeat seconds show command-options
```

Parameter	Description
seconds	Interval at which to re-enter the command. You can specify 1-300 seconds.
command-options	Options of the **show** command. See "Show Commands" on page 689.

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.

Example

The following command displays SLB TCP-stack statistics every 30 seconds:

```
AX#repeat 30 show slb tcp stack
Total
-------------------------------------------------------------------
Currently EST conns        29
Active open conns          6968
Passive open conns         7938
Connect attempt failures   0
Total in TCP packets       678804
Total out TCP packets      712974
Retransmitted packets      359
Resets rcvd on EST conn    5369
Reset Sent                 4303
Refreshing command every 30 seconds. (press ^C to quit) Elapsed Time: 00:00:00
Total
-------------------------------------------------------------------
Currently EST conns        30
Active open conns          6992
Passive open conns         7939
Connect attempt failures   0
Total in TCP packets       679433
Total out TCP packets      712986
Retransmitted packets      367
Resets rcvd on EST conn    5781
Reset Sent                 4305
Refreshing command every 30 seconds. (press ^C to quit) Elapsed Time: 00:00:30
```

show

Description Display system or configuration information. See “Show Commands” on page 689.

shutdown

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	Shutdown at a specific time/date (*hh*:*mm*)
in	Shutdown after time interval (*mm* or *hh*:*mm*)
cancel	Cancel pending shutdown
text	Reason for shutdown

Mode Privileged EXEC mode

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

```
AX#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]
AX#
```

Example The following command cancels a scheduled system shutdown:

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

ssh

Description Establish a Secure Shell (SSH) connection from the AX device to another device. (See “ssh” on page 55.)

telnet

Description

Establish a Telnet connection from the AX device to another device. (See “telnet” on page 56.)

terminal

Description

Set terminal display parameters.

Syntax

```
terminal option value
```

Parameter	Description
`auto-size`	Enables the terminal length and width to automatically change to match the terminal window size.
`editing`	Enables command-line editing.
`history [size]`	Enables and controls the command history function. The *size* option specifies the number of command lines that will be held in the history buffer. You can specify 0-1000.
`length num`	Sets the number of lines on a screen. You can specify 0-512. Specifying 0 disables pausing.
`monitor`	Copies debug output to the current terminal.
`width num`	Sets the width of the display terminal. You can specify 0-512. The setting 0 means “infinite”.

Default

The terminal settings have the following defaults:

- **auto-size** – enabled
- **editing** – enabled
- **history** – enabled; default size is 256
- **length** – 24
- **monitor** – disabled
- **width** – 80

Mode

Privileged EXEC mode or global configuration mode

Example

The following command changes the terminal length to 40:

```
AX#terminal length 40
```

traceroute

Description

Trace a route. See “traceroute” on page 57.

write

Description

Write the running-config to a configuration profile.

Syntax

```
write {memory | force}
[primary | secondary | profile-name] [cf]
```

Parameter	Description
`memory`	Writes (saves) the running-config to a configuration profile.
`force`	Forces the AX device to save the configuration regardless of whether the system is ready.
`primary`	Replaces the configuration profile stored in the primary image area with the running-config.
`secondary`	Replaces the configuration profile stored in the secondary image area with the running-config.
`cf`	Replaces the configuration profile in the specified image area (primary or secondary) on the compact flash rather than the hard disk. If you omit this option, the configuration profile in the specified area on the hard disk is replaced.

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.

Mode

Configuration mode

Usage

CAUTION! Using the **write force** command can result in an incomplete or empty configuration! A10 Networks recommends that you use this command only with the advice of A10 Networks Technical Support.

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

For more information about configuration profiles, see the *AX Series System Configuration and Administration Guide*.

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

```
AX#write memory primary
```

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

```
AX#write memory slbconfig2
```

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

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

Example The following commands attempt to save the running-config on a system that is not ready, then force the save operation to take place anyway:

```
AX#write memory
AX system is not ready. Cannot save the configuration.
AX#write force
```

write terminal

Description Display the running-config on the terminal.

Syntax `write terminal`

Mode Privileged EXEC mode or global configuration mode

Config Commands: Global

This chapter describes the commands for configuring global AX parameters.

To access this configuration level, enter the **configure** [**terminal**] command at the Privileged EXEC level.

To display global settings, use **show** commands. (See "Show Commands" on page 689.)

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See "backup system" on page 50 and "backup log" on page 48.
- **clear** – See "clear" on page 59.
- **debug** – See "debug" on page 64.
- **diff** – See "diff" on page 65.
- **export** – See "export" on page 67.
- **health-test** – See "health-test" on page 52.
- **help** – See "CLI Quick Reference" on page 35.
- **import** – See "import" on page 69.
- **repeat** – See "repeat" on page 74.
- **show** – See "Show Commands" on page 689.
- **write** – See "write" on page 77.

6rd

Description

Configure IPv6 Rapid Deployment (6rd). See "Config Commands: 6rd" on page 585.

access-list (standard)

Description

Configure 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}
source-ipaddr {filter-mask | /mask-length}
[log [transparent-session-only]]
```

Parameter	Description
acl-num	Standard ACL number. You can specify 1-99.
seq-num	Sequence number of this rule in the ACL. You can use this option to resequence the rules in the ACL.
deny | permit	Action to take for traffic that matches the ACL. **deny** – For ACLs applied to interfaces or used for management access, drops the traffic. **permit** – For ACLs applied to interfaces or used for management access, allows the traffic. For ACLS used for IP source NAT, 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.

Parameter	Description
l3-vlan-fwd-disable	Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
remark *string*	Adds a remark to the ACL. The remark appears at the top of the ACL when you display it in the CLI. 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.

`source-ipaddr {filter-mask | /mask-length}`

Denies or permits traffic received from the specified host or subnet. The *filter-mask* specifies the portion of the address to filter:

– Use 0 to match.

– Use 255 to ignore.

For example, the following *filter-mask* filters on a 24-bit subnet: 0.0.0.255

Alternatively, you can use *mask-length* to specify the portion of the address to filter. For example, you can specify "/24" instead "0.0.0.255" to filter on a 24-bit subnet.

`log [transparent-session-only]`

Configures the AX 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.

- To use an ACL to filter traffic on an interface, see "access-list" on page 203.
- To use an ACL to control management access, see "disable-management" on page 115 and "enable-management" on page 121.

- To use an ACL with source NAT, see “ip nat inside” on page 247.

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. (See “access-list (extended)” on page 82.)

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:

```
AX(config)#access-list 1 deny 10.10.10.0 0.0.0.255
AX(config)#interface ethernet 4
AX(config-if:ethernet4)#access-list 1 in
```

access-list (extended)

Description

Configure 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 |
  net-src-ipaddr {filter-mask | /mask-length}}

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

[fragments] [vlan vlan-id] [dscp num]

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

or

Syntax

```
[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 |
  net-src-ipaddr {filter-mask | /mask-length}}

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

[fragments] [vlan vlan-id] [dscp num]

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

or

Syntax

```
[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] [dscp num]
  [established]

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

Parameter	Description
acl-num	Extended ACL number. You can specify 100-199.
seq-num	Sequence number of this rule in the ACL. You can use this option to resequence the rules in the ACL.
deny | permit	Action to take for traffic that matches the ACL. **deny** – Drops the traffic. **permit** – Allows the traffic.
l3-vlan-fwd-disable	Disables Layer 3 forwarding between VLANs for IP addresses that match the ACL rule.
remark *string*	Adds a remark to the ACL. The remark appears at the top of the ACL when you display it in the CLI. To use blank spaces in the remark, enclose the entire remark string in double quotes. The ACL must already exist before you can configure a remark for it.
ip	Filters on IP packets.
icmp	Filters on ICMP packets.
tcp | udp	Filters on TCP or UDP packets. The **tcp** and **udp** options enable you to filter on protocol port numbers.
type *type-option*	This option is applicable if the protocol type is **icmp**. Matches based on the specified ICMP type. You can specify one of the following. Enter the type name or the type number (for example, **dest-unreachable** or **3**). **any-type** – Matches on any ICMP type. **dest-unreachable** | **3** – Type 3, destination unreachable **echo-reply** | **0** – Type 0, echo reply **echo-request** | **8** – Type 8, echo request **info-reply** | **16** – Type 16, information reply **info-request** | **15** – Type 15, information request **mask-reply** | **18** – Type 18, address mask reply

mask-request | **17** – Type 17, address mask request

parameter-problem | **12** – Type 12, parameter problem

redirect | **5** – Type 5, redirect message

source-quench | **4** – Type 4, source quench

time-exceeded | **11** – Type 11, time exceeded

timestamp | **13** – Type 13, timestamp

timestamp-reply | **14** – Type 14, timestamp reply

type-num – ICMP type number, 0-254

`code` *`code-num`*

This option is applicable if the protocol type is **icmp**. Matches based on the specified ICMP code.

any-code – Matches on any ICMP code.

code-num – ICMP code number, 0-254

`any` `|` **`host`** *`host-src-ipaddr`* `|` *`net-src-ipaddr`* `{`*`filter-mask`* `|` *`/mask-length`*`}`

Source IP address(es) to filter.

`any` – The ACL matches on all source IP addresses.

`host` *`host-src-ipaddr`* – The ACL matches only on the specified host IP address.

`net-src-ipaddr` `{`*`filter-mask`* `|` *`/mask-length`*`}` – The ACL matches on any host in the specified subnet. The *filter-mask* specifies the portion of the address to filter:

– Use 0 to match.

– Use 255 to ignore.

For example, the following *filter-mask* filters on a 24-bit subnet: 0.0.0.255

Alternatively, you can use *mask-length* to specify the portion of the address to filter. For example, you can specify “/24” instead “0.0.0.255” to filter on a 24-bit subnet.

eq *src-port* |
gt *src-port* |
lt *src-port* |
range *start-src-port*
end-src-port

For **tcp** or **udp**, the source protocol ports to filter.

eq *src-port* – The ACL matches on traffic from the specified source port.

gt *src-port* – The ACL matches on traffic from any source port with a higher number than the specified port.

lt *src-port* – The ACL matches on traffic from any source port with a lower number than the specified port.

range *start-src-port end-src-port* – The ACL matches on traffic from any source port within the specified range.

any |
host *host-dst-ipaddr* |
net-dst-ipaddr
{*filter-mask* |
/mask-length}

Destination IP address(es) to filter.

eq *dst-port* |
gt *dst-port* |
lt *dst-port* |
range *start-dst-port*
end-dst-port

For **tcp** or **udp**, the destination protocol ports to filter.

fragments

Matches on packets in which the More bit in the header is set (1) or has a non-zero offset.

vlan *vlan-id*

Matches on the specified VLAN. VLAN matching occurs for incoming traffic only.

dscp *num*

Matches on the 6-bit Diffserv value in the IP header, 1-63.

established

Matches on TCP packets in which the ACK or RST bit is not set. This option is useful for protecting against attacks from outside. Since a TCP connection from the outside does not have the ACK bit set (SYN only), the connection is dropped. Similarly, a connection established from the inside always has the ACK bit set. (The

	first packet to the network from outside is a SYN/ACK.)
`log [transparent-session-only]`	Configures the AX 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:

- To use an ACL to filter traffic on an interface, see “access-list” on page 203.
- To use an ACL to control management access, see “disable-management” on page 115 and “enable-management” on page 121.
- To use an ACL with source NAT, see “ip nat inside” on page 247.

accounting

Description

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

- EXEC accounting – provides information about EXEC terminal sessions (user shells) on the AX device.

- Command accounting – provides information about the EXEC shell commands executed under a specified privilege level. This command also allows you to specify the debug level.

Syntax

```
[no] accounting exec {start-stop | stop-only}
{radius | tacplus}

[no] accounting commands cmd-level stop-only
tacplus

[no] accounting debug debug-level
```

Parameter	Description
start-stop	Sends an Accounting START packet to TACACS+ servers when a user establishes a CLI session, and an Accounting STOP packet when the user logs out or the session times out.
stop-only	Only sends an Accounting STOP packet when the user logs out or the session times out.
radius | tacplus	Specifies the type of accounting server to use.
cmd-level	Specifies which level of commands will be accounted. The commands are divided into the following levels: 15(admin) – Commands available for admin (all commands) 14(config) – Commands available in config mode (not include the command of “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 are the same as command level 1.
debug-level	Specifies the debug level for accounting. The debug level is set as flag bits for different types of debug messages. The AX 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 AX, 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 The accounting server also must be configured. See “radius-server” on page 157 or “tacacs-server” on page 191.

Example The following command configures the AX device to send an Accounting START packet to the previously defined TACACS+ servers when a user establishes a CLI session on the device. The AX device also will send an Accounting STOP packet when a user logs out or their session times out.

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

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

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

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

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

The following command specifies debug level 15 for accounting.

```
AX(config)#accounting debug l5
```

admin

Configure an admin account for management access to the AX Series device.

Syntax

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

Parameter	Description
admin-username	Admin username, 1-31 characters.

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 management interfaces through which the admin is allowed to access the AX device.

Note: The **axapi** option is not applicable to IPv6 migration.

Command	Description
admin	Enters the configuration level for another admin account. If you are configuring multiple admin accounts, this command simplifies navigation of the CLI because you do not need to return to the Configuration mode level to begin configuration of the next account.
disable	Disables the admin account.
enable	Enables the admin account.
password *string*	Sets the password, 1-63 characters. Passwords are case sensitive and can contain special characters. (For more information, see "Special Character Support in Strings" on page 43.)
privilege *priv-level*	Sets the privilege level for the account. **read** – The admin can access the User EXEC and Privileged EXEC levels of the CLI only. **write** – The admin can access all levels of the CLI.

ssh-pubkey *options*

Manage public key authentication for the admin.

ssh-pubkey import *url* – Imports the public key onto the AX device.

The *url* specifies the file transfer protocol, username (if required), and directory path.

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long.

To enter the entire URL:

```
tftp://host/file
ftp://[user@]host[:port]/file
scp://[user@]host/file
rcp://[user@]host/file
```

ssh-pubkey delete *num* – Deletes a public key. The *num* option specifies the key number on the AX device. The key numbers are displayed along with the keys themselves by the **ssh-pubkey list** command. (See below.)

ssh-pubkey list – Verifies installation of the public key.

(For information about creating the public key, see the “Management Security Features” chapter of the *AX Series System Configuration and Administration Guide*.)

trusted-host *ipaddr* {*subnet-mask* | /*mask-length*}

Specifies the host or subnet address from which the admin is allowed to log onto the AX device.

unlock

Unlocks the account. Use this option if the admin has been locked out due to too many login attempts with an incorrect password. (To configure lockout parameters, see “admin lockout” on page 93.)

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 admin accounts have the following defaults:

- **access** – Access is allowed through the CLI, GUI, and aXAPI interfaces.
- **enable** / **disable** – Admin accounts are enabled by default as soon as you add them.
- **password** – "a10". This is the default for the "admin" account and for any admin account you configure if you do not configure the password for the account.
- **privilege** – **read**
- **trusted-host** – 0.0.0.0 /0, which allows access from any host or subnet.
- **unlock** – N/A. Admin accounts are unlocked by default. They can become locked based on **admin lockout** settings.

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 commands add admin "adminuser1" with password "1234":

```
AX(config)#admin adminuser1
AX(config-admin:adminuser1)#password 1234
```

Example

The following commands add admin "adminuser2" with password "12345678" and write privilege:

```
AX(config)#admin adminuser2
AX(config-admin:adminuser2)#password 12345678
AX(config-admin:adminuser2)#write
```

Example

The following commands add admin "adminuser3" with password "abcdefgh" and write privilege, and restrict login access to the 10.10.10.x subnet only:

```
AX(config)#admin adminuser3
AX(config-admin:adminuser3)#password abcdefgh
AX(config-admin:adminuser3)#write
AX(config-admin:adminuser3)#trusted-host 10.10.10.0 /24
```

Example

The following commands deny management access by admin “admin2” using the CLI:

```
AX(config)#admin admin2
AX(config-admin:admin2)#no access cli
```

admin lockout

Description

Set lockout parameters for admin sessions.

Syntax

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

Parameter	Description
`duration` *`minutes`*	Number of minutes a lockout remains in effect. After the lockout times out, the admin can try again to log in. You can specify 0-1440 minutes. To keep accounts locked until you or another authorized administrator unlocks them, specify 0.
`enable`	Enables the lockout feature.
`reset-time` *`minutes`*	Number of minutes the AX device remembers failed login attempts. You can specify 1-1440 minutes.
`threshold` *`number`*	Number of consecutive failed login attempts allowed before an administrator is locked out. You can specify 1-10.

Default

The lockout feature is disabled by default. This command has the following defaults:

- **duration** – 10 minutes
- **reset-time** – 10 minutes
- **threshold** – 5

Example

The following command enables admin lockout:

```
AX(config)#admin lockout enable
```

arp

Description Create a static ARP entry or change the timeout for dynamic entries.

Syntax

```
[no] arp ipaddr mac-address
[interface ethernet number
[vlan vlan-id]]
```

Parameter	Description
ipaddr	IP address of the static entry.
mac-address	MAC address of the static entry.
number	Specifies the Ethernet data interface.
vlan *vlan-id*	If the AX 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

arp timeout

Description Change the aging timer for dynamic ARP entries.

Syntax

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

Parameter	Description
seconds	Number of seconds a dynamic entry can remain unused before being removed from the ARP table. You can specify 60-86400 seconds.

Default 300 seconds (5 minutes)

Mode Configuration mode

audit

Description

Configure command auditing.

Syntax

```
[no] audit enable [privilege]
```

```
[no] audit size num-entries
```

Parameter	Description
enable [**privilege**]	Enables command auditing. The **privilege** option enables logging of Privileged EXEC commands also. Without this option, only configuration commands are logged.
size *num-entries*	Specifies the number of entries the audit log file can hold. You can specify 1000-30000 entries. When the log is full, the oldest entries are removed to make room for new entries.

Default

Command auditing is disabled by default. 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 logins and logouts 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)
- HA configuration synchronization

The audit log is maintained in a separate file, apart from the system log.

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

authentication

Description

Set the authentication method used to authenticate administrative access to the AX.

Syntax

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

Syntax

```
[no] authentication disable-local
```

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 *method1* [*method2*]	Specifies the authentication method to use. Optionally, you can specify a backup method (*method2*). Each method can be one of the following: **local** – Uses the AX 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.
disable-local	Disables automatic local authentication of the “admin” account. Without this option, the “admin” account is always authenticated locally, regardless of the authentication configuration used for the other admin accounts.

Default

By default, only local authentication is used.

Mode

Configuration mode

Usage

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.

The authentication server(s) also must be configured. See “radius-server” on page 157 or “tacacs-server” on page 191.

If the RADIUS or TACACS+ server responds, the local database is not checked.

- If the admin name and password are found on the RADIUS or TACACS+ server, the admin is granted access.
- If the admin name and password are not found on the RADIUS or TACACS+ server, the admin is denied access.

Only if there is no response from any RADIUS or TACACS+ server, does the AX device check its local database for the admin name and password.

Note: An exception is made for the “admin” account. By default, the AX device always uses local authentication for “admin”. You can use the **disable-local** option to disable automatic local authentication for “admin”, in which case the authentication process is the same as for other admin accounts.

Example

The following commands configure a pair of RADIUS servers and configure the AX 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.

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

authorization

Description

Configure authorization for controlling access to functions in the CLI. The AX 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
cmd-level	Specifies the level of commands that will be authorized. The commands are divided into the following levels: 15(admin) – This is the most extensive level of authorization. Commands at all CLI levels, including those used to configure admin accounts, are sent to TACACS+ for authorization. 14(config) – Commands at all CLI levels ***except*** those used to configure admin accounts are sent to TACACS+ for authorization. Commands for configuring admin accounts are automatically allowed. 1(priv EXEC) – Commands at the Privileged EXEC and User EXEC levels are sent to TACACS+ for authorization. Commands at other levels are automatically allowed. 0 (user EXEC) – Commands at the User EXEC level are sent to TACACS+ for authorization. Commands at other levels are automatically allowed. Command levels 2-13 are equivalent to command level 1.
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-level	Specifies the debug level for authorization. The debug level is set as flag bits for different types of debug messages. The AX Series 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 AX Series 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 The authorization server also must be configured. See "radius-server" on page 157 or "tacacs-server" on page 191.

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.

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

The following command specifies debug level 15 for authorization:

```
AX(config)#authorization debug l5
```

axdebug

Description Access the AX debug subsystem. See "AX Debug Commands" on page 789.

backup periodically

Description Schedule periodic backups.

Caution: **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 periodically {system | log}
{hour num | day num | week num}
[use-mgmt-port] url
```

Parameter	Description
`system`	Backs up the following system files: – Startup-config files – Admin accounts and login and enable passwords – Class 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.
`log`	Backs up the system log.
`hour` *`num`* | **`day`** *`num`* | **`week`** *`num`*	Specifies how often to perform the back ups. You can specify one of the following: **hour** *num* – Performs the backup each time the specified number of hours passes. For example, specifying **hour 3** causes the backup to occur every 3 hours. You can specify 1-65534 hours. There is no default. **day** *num* – Performs the backup each time the specified number of days passes. For example, specifying **day 5** causes the backup to occur every 5 days. You can specify 1-199 days. There is no default. **week** *num* – Performs the backup each time the specified number of weeks passes. For example, specifying **week 4** causes the backup to occur every 4 weeks. You can specify 1-199 weeks. There is no default.
`use-mgmt-port`	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. Without this option, the AX device attempts to use the data route table to reach the remote device through a data interface.
`url`	Specifies the file transfer protocol, username (if required), and directory path to which to save the backups.

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long.

To enter the entire URL:

tftp://*host*/*file*

ftp://[*user*@]*host*[:*port*]/*file*

scp://[*user*@]*host*/*file*

rcp://[*user*@]*host*/*file*

Default Not set

Mode Configuration mode

Example The following commands schedule weekly backups of the entire system, verify the configuration, and save the backup schedule to the startup-config:

```
AX(config)#backup periodically system week 1 ftp:
Address or name of remote host []?10.10.10.4
User name []?admin2
Password []?********
File name [/]?weekly-sys-backup
AX(config)#show backup
backup periodically system hour 168 ftp://admin2@10.10.10.4//weekly-sys-backup
Next backup will occur at 14:37:00 PDT Thu Aug 19 2010
AX(config)#write memory
Building configuration...
[OK]
```

banner

Set the banners to be displayed when an admin logs onto the CLI or accesses the Privileged EXEC mode.

Syntax Description [**no**] **banner** {**exec** | **login**} [**multi-line** *end-marker*] *line*

Parameter	Description
exec	Configures the EXEC mode banner.
login	Configures the login banner.

multi-line *end-marker*	Hexadecimal number to indicate the end of a multi-line message. The end marker is a simple string up to 2-characters long, each of the which must be an ASCII character from the following range: 0x21-0x7e. The multi-line banner text starts from the first line and ends at the marker. If the end marker is on a new line by itself, the last line of the banner text will be empty. If you do not want the last line to be empty, put the end marker at the end of the last non-empty line.
line	Specifies the banner text.

Default

The default login banner is as follows: “Welcome to AX”

The default EXEC banner is as follows: “[type ? for help]”

Mode

Configuration mode

Example

The following examples set the login banner to “welcome to login mode” and set the EXEC banner to a multi-line greeting:

```
AX(config)#banner exec welcome to exec mode
AX(config)#banner login multi-line bb
Enter text message, end with string 'bb'.
Here is a multi-line
Greeting.
bb
AX(config)#
```

bfd echo

Description

Enables echo support for Bidirectional Forwarding Detection (BFD).

Syntax

```
[no] bfd echo
```

Default

Disabled

Mode

Configuration mode

Usage

BFD echo enables a device to test data path to the neighbor and back. When a device generates a BFD echo packet, the packet uses the routing link to the neighbor device to reach the device. The neighbor device is expected to send the packet back over the same link.

bfd enable

Description Enable Bidirectional Forwarding Detection (BFD) on a global basis.

Syntax

```
[no] bfd {echo | enable | interval}
```

Parameter	Description
echo	Globally enables the echo function. When the **echo** option is enabled, the detection interval, (or the time that the AX device waits for a BFD control packet from a BFD neighbor), is set automatically to 3200 ms.
enable	Globally enable BFD packet processing.
interval [*ms*] **min-rx** [*ms*] **multiplier**	Transmit interval between BFD packets. The *ms* option allows you to specify a value from 48-1000 milliseconds. The **multiplier** option is a value used to multiply the interval and can range from 3-50.

Default Disabled

Mode Configuration mode

bfd interval

Description Configure BFD timers.

Syntax

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

Parameter	Description
interval *ms*	Rate at which the AX device sends BFD control packets to its BFD neighbors. You can specify 48-1000 milliseconds (ms).
min-rx *ms*	Minimum amount of time in milliseconds that the AX device waits to receive a BFD control packet from a BFD neighbor. If a control packet is not received within the specified time, the multiplier (below) is incremented by 1. You can specify 48-1000 ms. The default is 800 ms.
multiplier *num*	Maximum number of consecutive times the AX device will wait for a BFD control packet from a

neighbor. If the multiplier value is reached, the AX device concludes that the routing process on the neighbor is down. You can specify 3-50.

Default

The BFD timers have the following defaults:

- **interval** – 800 ms
- **min-rx** – 800 ms
- **multiplier** – 4

Mode

Configuration mode

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.

bgp extended-asn-cap

Description

Enable the AX device to send 4-octet BGP Autonomous System Number (ASN) capabilities.

Syntax

```
[no] bgp extended-asn-cap
```

Default

Disabled; 2-octet ASN capabilities are enabled instead.

Mode

Configuration mode

Usage

To configure other BGP parameters, see "Config Commands: Router – BGP" on page 395.

bgp nexthop-trigger

Description

Configure BGP nexthop tracking.

Syntax

```
[no] bgp nexthop-trigger delay seconds

[no] bgp nexthop-trigger enable
```

Parameter	Description
`delay seconds`	Specifies the how long BGP waits before walking the full BGP table to determine which prefixes are affected by the nexthop changes, after receiving a trigger about nexthop changes. You can specify 1-100 seconds.
`enable`	Enables nexthop tracking.

Default

BGP nexthop tracking is disabled by default. When you enable it, the default delay is 5 seconds.

Mode

Configuration mode

Usage

To configure other BGP parameters, see "Config Commands: Router – BGP" on page 395.

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 | hd`	Medium to be repaired: **cf** – compact flash **hd** – hard disk

Default

N/A

Mode

Configuration mode

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 AX Series is rebooted.

Syntax

```
bootimage {both | cf | hd} {pri | sec}
```

Parameter	Description
`cf | hd`	Boot medium. The AX Series 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

Example The following command configures the AX Series to boot from the secondary image area on the hard disk the next time the device is rebooted:

```
AX(config)#bootimage hd sec
```

bpdu-fwd-group

Description Configure a group of tagged Ethernet interfaces for forwarding Bridge Protocol Data Units (BPDUs). BPDU forwarding groups enable you to use the AX 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
```

Parameter	Description
group-num	BPDU forwarding group number, 1-8.

This command changes the CLI to the configuration level for the BPDU forwarding group, where the following command is available.

Command	Description
`[no] ethernet portnum [to portnum] [ethernet portnum] ...`	Ethernet interfaces 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:

```
AX(config)#bpdu-fwd-group 1
AX(config-bpdu-fwd-group:1)#ethernet 1 to 3
AX(config-bpdu-fwd-group:1)#show bpdu-fwd-group
BPDU forward Group 1 members: ethernet 1 to 3
```

bridge-vlan-group

Description

Configure a bridge VLAN group for VLAN-to-VLAN bridging.

Syntax

```
[no] bridge-vlan-group group-num
```

Parameter	Description
group-num	Bridge VLAN group number.

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 | forward-ip-traffic	Specifies the types of traffic the bridge VLAN group is allowed to forward: **forward-all-traffic** – This option forwards all types of traffic. **forward-ip-traffic** – This option includes typical traffic between end hosts, such as ARP requests and responses.

[no] name *string*	Specifies a name for the group. The string can be 1-63 characters long. If the string contains blank spaces, use double quotation marks around the entire string.
[no] router-interface ve *num*	Adds a Virtual Ethernet (VE) interface to the group. This command is applicable only on AX devices deployed in gateway mode. The VE number must be the same as the lowest numbered VLAN in the group.
[no] vlan *vlan-id* [**vlan** *vlan-id* ... | **to vlan** *vlan-id*]	Adds VLANs to the group.

Default

By default, the configuration does not contain any bridge VLAN groups. When you create a bridge VLAN group, it has the following default settings:

- **forward-all-traffic** | **forward-ip-traffic** – **forward-ip-traffic**
- **name** – Not set
- **router-interface** – Not set
- **vlan** – Not set

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.

Example

For more information, including configuration notes and examples, see the “VLAN-to-VLAN Bridging” chapter in the *AX Series System Configuration and Administration Guide*.

class-list (for many pools, standard NAT)

Description

Configure IP class lists for deployment that use a large number of NAT pools.

Note: This section describes how to configure a class list for standard Network Address Translation (NAT). For information about using class lists to configure IPv6 migration features, see "class-list (for IPv6 migration features)" on page 110.

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a file.

This command changes the CLI to the configuration level for the specified class list, where the following commands are available.

(The other commands are common to all CLI configuration levels. See "Config Commands: Global" on page 79.)

Command	Description
[**no**] *ipaddr /network-mask* **glid** *num*	Specifies the inside subnet that requires NAT. The *network-mask* specifies the network mask. 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. The **glid** *num* option specifies the global LID that refers to the pool.

Default

None

Mode

Configuration mode

Usage

First configure the IP pools. Then configure the global LIDs. In each global LID, use the **use-nat-pool** *pool-name* command to map clients to the pool. Then configure the class list entries.

As an alternative to configuring class entries on the AX device, you can configure the class list using a text editor on another device, then import the class list onto the AX device. To import a class list, see “import” on page 69.

Example

See the “Configuring Dynamic IP NAT with Many Pools” section in the “Network Address Translation” chapter of the *AX Series System Configuration and Administration Guide*.

class-list (for IPv6 migration features)

Description

For information about the class-list syntax applicable to IPv6 migration features, see the following sections:

- “class-list (for LSN)” on page 455
- “class-list (for NAT64)” on page 526
- “class-list (for DS-Lite)” on page 551

clock timezone

Set the clock timezone.

Syntax Description

```
clock timezone timezone [nodst]
```

Parameter	Description
timezone	Timezone to use. To view the available timezones, enter the following command: **clock timezone ?**
nodst	Disables Daylight Savings Time.

Default

Europe/Dublin (GMT)

Mode

Configuration mode

Usage

If you use the GUI or CLI to change the AX 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. For example, in the GUI, the graphs displayed on the Monitor > Overview page are cleared.

Example The following commands list the available timezones, then set the timezone to America/Los_Angeles:

```
AX(config)#clock timezone ?
Pacific/Midway               (GMT-11:00)Midway Island, Samoa
Pacific/Honolulu             (GMT-10:00)Hawaii
America/Anchorage            (GMT-09:00)Alaska
...
AX(config)#clock timezone America/Los_Angeles
```

convert-passwd

Description Convert admin accounts and enable passwords into pre-1.2.7 format before downgrade to AX Release 1.2.6 or earlier.

Syntax

```
convert-passwd {pri | sec}
```

Parameter	Description
pri | sec	Specifies the image area to which you want to save the admin accounts and passwords. Specify the image area from which you to plan to boot using the 1.2.6 or earlier image.

Default N/A

Mode Configuration mode

Usage Use this command ***only*** if you are planning to downgrade to AX Release 1.2.6 or earlier. Use the command ***before*** you downgrade.

In AX Release 1.2.7 and later, the AX device maintains all admin accounts and enable passwords in a single file, which applies to both the primary and secondary image areas. In software releases prior to 1.2.7, the AX device maintained separate files for the primary and secondary image areas. During runtime, the AX device used the admin accounts and enable passwords that were in the file corresponding to the image area from which the device was booted.

To keep the new admin accounts and enable passwords, perform the following steps ***before you downgrade***:

1. Log onto the CLI, with an admin account that has Root or global Read-Write (Super User) privileges.

2. Save the configuration (**write memory**), to save any new or changed admin accounts or passwords. (If you perform step 2 without first saving

the configuration, any unsaved admin account or password changes will be lost.)

3. Use the following command at the Configuration mode level of the CLI:

   ```
   convert-passwd {pri | sec}
   ```

   The **pri** | **sec** option specifies the image area to which you want to save the admin accounts and passwords. Specify the image area from which you to plan to boot using the 1.x image.

copy

Copy a running-config or startup-config.

Syntax Description

```
copy {running-config | startup-config |
from-profile-name}
[use-mgmt-port]
{url | to-profile-name [cf]}
```

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.
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 AX device attempts to use the data route table to reach the remote device through a data interface.
url	Copies the running-config or configuration profile to a remote device. The URL specifies the file transfer protocol, username, and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long.

To enter the entire URL:

tftp://*host*/*file*

ftp://[*user*@]*host*[:*port*]/*file*

scp://[*user*@]*host*/*file*

rcp://[*user*@]*host*/*file*

from-profile-name Configuration profile you are copying from.

to-profile-name [**cf**] Configuration profile you are copying to. The **cf** option copies the profile to the compact flash instead of the hard disk.

Note: Copying a profile from the compact flash to the hard disk is not supported.

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 AX device most recently rebooted.

Default None

Mode Configuration mode

Usage If you are planning to configure a new AX device by loading the configuration from another AX device:

1. On the configured AX device, use the **copy startup-config** *url* command to save the startup-config to a remote server.
2. On the new AX device, use the **copy** *url* **startup-config** command to copy the configured AX device's startup-config from the remote server onto the new AX device.
3. Use the **reboot** command (at the Privileged EXEC level) to reboot the new AX 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 AX 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 AX device:

```
AX(config)#copy startup-config slbconfig3
```

debug

Note: A10 Networks Technical Support recommends using the AXdebug commands instead of the **debug** command. (See “AX Debug Commands” on page 789.)

delete startup-config

Description Delete a locally stored configuration profile.

Syntax

```
delete startup-config profile-name [cf]
```

Parameter	Description
profile-name	Configuration profile name.
cf	Deletes the specified profile from compact flash instead of the hard disk. If you omit this option, the profile is deleted from the hard disk.

Default N/A

Mode Configuration mode

Usage Although the command uses the **startup-config** option, the command only deletes the configuration profile linked to “startup-config” if you enter that profile’s name. The command deletes only the profile you specify.

If the configuration profile you specify is linked to “startup-config”, “startup-config” is automatically relinked to the default. (The default is the configuration profile stored in the image area from which the AX device most recently rebooted).

Example The following command deletes configuration profile “slbconfig2”:

```
AX(config)#delete startup-config slbconfig2
```

disable

Description Disable real or virtual servers.

Syntax

```
disable slb server [server-name] [port port-num]

disable slb virtual-server [server-name]
[port port-num]
```

Parameter	Description
server-name	Disables the specified real or virtual server.
port *port-num*	Disables only the specified service port. If you omit the *server-name* option, the port is disabled on all real or virtual servers. Otherwise, the port is disabled only on the server you specify.

Default Enabled

Mode Configuration mode

Example The following command disables all virtual servers:

```
AX(config)#disable slb virtual-server
```

Example The following command disables port 80 on all real servers:

```
AX(config)#disable slb server port 80
```

Example The following command disables port 8080 on real server “rs1”:

```
AX(config)#disable slb server rs1 port 8080
```

disable-management

Description Disable management access to the AX Series device.

Syntax

```
[no] disable-management service
{all | ssh | telnet | http | https | snmp | ping}
{management | ethernet port-num [to port-num] |
 ve ve-num [to ve-num]}
```

or

Syntax

```
[no] disable-management service acl acl-num
{management | ethernet port-num [to port-num] |
 ve ve-num [to ve-num]}
```

Parameter	Description
all	Disables access to all the management services listed in Table 1.
ssh	Disables SSH access to the CLI.
telnet	Disables Telnet access to the CLI.
http	Disables HTTP access to the management GUI.

https Disables HTTPS access to the management GUI.

snmp Disables SNMP access to the AX device's SNMP agent.

ping Disables ping replies from AX interfaces. This option does not affect the AX device's ability to ping other devices.

acl *acl-num* Permits or denies management access based on permit or deny rules in the ACL.

management | **ethernet** *port-num* [**to** *port-num*] | **ve** *ve-num* [**to** *ve-num*] Specifies the interfaces for which you are configuring access control.

Note: Disabling **ping** replies from being sent by the device does not affect the device's ability to ping other devices.

Default Table 1 lists the default settings for each management service.

TABLE 1 Default Management Access

Management Service	Ethernet Management Interface	Ethernet and VE Data Interfaces
SSH	Enabled	Disabled
Telnet	Disabled	Disabled
HTTP	Enabled	Disabled
HTTPS	Enabled	Disabled
SNMP	Enabled	Disabled
Ping	Enabled	Enabled

Mode Configuration mode

Usage If you disable the type of access you are using on the interface you are using at the time you enter this command, your management session will end. If you accidentally lock yourself out of the device altogether (for example, if you use the **all** option for all interfaces), you can still access the CLI by connecting a PC to the AX device's serial port.

To enable management access, see "enable-management" on page 121.

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.

Notes Regarding Use of ACLs

If you use an ACL to secure management access, the action in the ACL rule that matches the management traffic's source address is used to permit or deny access, regardless of other management access settings.

For example, if you disable Telnet access to a data interface, but you also enable access to the interface using an ACL with permit rules, the ACL permits Telnet (and all other) access to the interface, for traffic that matches the permit rules in the ACL.

If you want certain types of management access to be disabled on an interface, do not use a permit ACL to control management access to the interface.

Each ACL has an implicit **deny any any** rule at the end. If the management traffic's source address does not match a permit rule in the ACL, the implicit **deny any any** rule is used to deny access.

On data interfaces, you can disable or enable access to specific services and also use an ACL to control access. However, on the management interface, you can disable or enable access to specific services ***or*** control access using an ACL, but you can not do both.

Example

The following command disables HTTP access to the out-of-band management interface:

```
AX(config)#disable-management service http management
You may lose connection by disabling the http service.
Continue? [yes/no]:yes
```

do

Description

Run a Privileged EXEC level command from a configuration level prompt, without leaving the configuration level.

Syntax

do *command*

Default

N/A

Mode

Configuration mode

Usage For information about the Privileged EXEC commands, see "Privileged EXEC mode Commands" on page 59.

Example The following command runs the **traceroute** command from the Configuration mode level:

```
AX(config)#do traceroute 10.10.10.9
```

ds-lite

Description Configure Dual-Stack Lite (DS-Lite). See "Config Commands: DS-Lite" on page 551.

enable

Description Enable real or virtual servers.

Syntax

```
enable slb server [server-name] [port port-num]

enable slb virtual-server [server-name]
[port port-num]
```

Parameter	Description
server-name	Enables the specified real or virtual server.
port *port-num*	Enables only the specified service port. If you omit the *server-name* option, the port is enabled on all real or virtual servers. Otherwise, the port is enabled only on the server you specify.

Default Enabled

Mode Configuration mode

Example The following command enables all virtual servers:

```
AX(config)#enable slb virtual-server
```

Example The following command enables port 80 on all real servers:

```
AX(config)#enable slb server port 80
```

Example The following command enables port 8080 on real server "rs1":

```
AX(config)#enable slb server rs1 port 8080
```

enable-core

Description Change the file size of core dumps.

Syntax

```
[no] enable-core [a10]
```

Parameter	Description
`a10`	Enables A10 core dump files. Without this option, system core dump files are used instead. System core dump files are larger than A10 core dump files.

Default If HA is configured, system core dump files are enabled by default. If HA is not configured, A10 core dump files are enabled by default.

Mode Configuration mode

enable-def-vlan-l2-forwarding

Description Enable Layer 2 forwarding on the default VLAN (VLAN 1).

Syntax

```
[no] enable-def-vlan-l2-forwarding
```

Default Layer 2 forwarding is disabled on VLAN 1, on AX devices deployed in route mode.

Mode Configuration mode

Usage This command applies only to routed mode deployments.

On a new or unconfigured AX 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 AX device itself (ex: LACP, HA, OSPF) 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 AX device has a single IP address for all data interfaces, Layer 2 forwarding is left enabled by default on VLAN 1.

enable-jumbo

Description

Globally enable jumbo frame support. In this release, a jumbo frame is an Ethernet frame that is more than 1522 bytes long.

Syntax

```
[no] enable-jumbo
```

Note: This is the only command required to enable jumbo support on FPGA models. See the Usage section below for details on enabling jumbo support on non-FPGA models.

Default

Disabled

Mode

Configuration mode

Introduced in Release

2.6.6-P4

Usage

Notes:

- 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 FPGA models only, for any incoming jumbo frame, if the outgoing MTU is less than the incoming frame size, the AX 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.
- Jumbo frames are not supported on model AX 1030, AX 2500, or AX2600.

If you are enabling jumbo support on a non-FPGA model, you must follow the **enable-jumbo** command with the **write-memory** command to save the configuration, and then use the **reboot** command at the Privileged EXEC level to reboot.

On non-FPGA models, after you enable (or disable) jumbo frame support, you must save the configuration and reboot to place the change into effect.

If jumbo support is enabled on a non-FPGA model and you erase the startup-config, the device is rebooted after the configuration is erased.

enable-management

Description

Enable management access to the AX Series device.

Syntax

```
[no] enable-management service
{all | ssh | telnet | http | https | snmp | ping}
{management | ethernet port-num [to port-num] |
 ve ve-num [to ve-num]}
```

or

Syntax

```
[no] enable-management service acl acl-num
{management | ethernet port-num [to port-num] |
 ve ve-num [to ve-num]}
```

Parameter	Description
all	Enables access to all the management services listed in Table 1.
ssh	Enables SSH access to the CLI.
telnet	Enables Telnet access to the CLI.
http	Enables HTTP access to the management GUI.
https	Enables HTTPS access to the management GUI.
snmp	Enables SNMP access to the AX device’s SNMP agent.
ping	Enables ping replies from AX interfaces. This option does not affect the AX device’s ability to ping other devices.
acl *acl-num*	Permits or denies management access based on permit or deny rules in the ACL.

management | **ethernet** *port-num* [**to** *port-num*] | **ve** *ve-num* [**to** *ve-num*]	Specifies the interfaces for which you are configuring access control.

Default Table 2 lists the default settings for each management service.

TABLE 2 Default Management Access

Management Service	Management Interface	Data Interfaces
SSH	Enabled	Disabled
Telnet	Disabled	Disabled
HTTP	Enabled	Disabled
HTTPS	Enabled	Disabled
SNMP	Enabled	Disabled
Ping	Enabled	Enabled

Mode Configuration mode

Usage See the "Usage" section in "disable-management" on page 115.

Example The following command enables Telnet access to Ethernet data interface 6:

```
AX(config)#enable-management service telnet ethernet 6
```

enable-password

Description Set the enable password, which secures access to the Privileged EXEC level of the CLI.

Syntax

```
[no] enable-password password-string
```

Parameter	Description
password-string	Password string, 1-63 characters. Passwords are case sensitive and can contain special characters. (For more information, see "Special Character Support in Strings" on page 43.)

Default By default, the password is blank. (Just press Enter.)

Mode Configuration mode

Example The following command sets the Privileged EXEC password to “execadmin”:

```
AX(config)#enable-password execadmin
```

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:

```
AX(config)#end
AX#
```

erase

Description Erase the startup-config file**.**

Syntax **erase**

Default N/A

Mode Configuration mode

Usage The “**no**” form of this command is not valid.

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.

```
AX(config)#erase
```

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:

```
AX(config)#exit
AX#
```

extended-stats

Description

Globally enable collection of SLB peak connection statistics.

Syntax

```
[no] extended-stats
```

Default

Disabled

Mode

Configuration mode

fixed-nat

Description

Configure Fixed-NAT. (See “Config Commands: Fixed-NAT” on page 609.)

floating-ip

Description Set a virtual IP address in a High-Availability configuration.

Syntax

```
[no] floating-ip ipaddr ha-group group-id
```

Parameter	Description
ipaddr	Virtual IP address of the HA group.
group-id	HA group ID.

Default None

Mode Configuration mode

Usage Use this command to specify the IP address of a next-hop upstream or downstream router used by real servers. (Also see "Config Commands: High Availability" on page 669.)

A floating IP address can not be the same as an address that already belongs to a device. For example, the IP address of an AX interface can not be a floating IP address.

Example The following commands configure 2 floating IPv6 addresses for HA group 1. Each floating IPv6 address is assigned to a specific IPv6 link-local data interface.

```
AX(config)#floating-ip fe80::def ha-group 1 ethernet 1
AX(config)#floating-ip fe80::de2 ha-group 1 ve 200
```

glid

Description Configure a Global Limit ID (GLID) to specify a NAT64 override action. See "glid (for NAT64 override)" on page 529.

Note: For information about using a GLID for standard NAT, see "class-list (for many pools, standard NAT)" on page 109.

ha

Description Configure High-Availability (HA) parameters. See "Config Commands: High Availability" on page 669.

health external

Use an external program for health monitoring.

Syntax

```
health external
{delete program-name |
import [use-mgmt-port] [description] url |
export [use-mgmt-port] program-name url}
```

Parameter	Description
program-name	Program file name, 1-31 characters.
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 AX device attempts to use the data route table to reach the remote device through a data interface.
description	Description of the program file, 1-63 characters.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp://***host***/***program-name* **ftp://**[*user***@**]*host*[**:***port*]**/***program-name* **scp://**[*user***@**]*host***/***program-name* **rcp://**[*user***@**]*host***/***program-name*

Default

N/A

Mode

Configuration mode

Usage

There is no "**no**" form of this command. To use an imported program for health monitoring, you also must configure a health method and apply the method to the server ports you want to monitor. See the description of the **external** option for "method" on page 664.

Example

The following example imports external program “mail.tcl” from FTP server 192.168.0.1:

```
AX(config)#health external import "checking mail server"
ftp://192.168.0.1/mail.tcl
```

health global

Description

Globally change health monitor parameters.

Syntax

```
health global
     {
     interval seconds |
     retry number |
     timeout seconds |
     up-retry number
     }
```

Parameter	Description
`interval` *seconds*	Number of seconds between health check attempt, 1-180 seconds. A health check attempt consists of the AX 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. Default is 5 seconds.
`retry` *number*	Maximum number of times the AX Series will send the same health check to an unresponsive server before determining that the server is down. You can specify 1-5. Default is 3.
`timeout` *seconds*	Number of seconds the AX Series waits for a reply to a health check, 1-12 seconds. Default is 5 seconds.
`up-retry` *number*	Number of consecutive times the device must pass the same periodic health check, in order to be marked Up. You can specify 1-10. The default is 1.

Note: The **timeout** parameter is not applicable to external health monitors.

You can change one or more parameters on the same command line.

Default

See above.

Note: To change a global parameter back to its factory default, use the **health global** form of the command and specify the parameter value to use.

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.

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: Global health monitor parameter changes automatically apply to all new health monitors configured after the change. To apply a global health monitor parameter change to health monitors that were configured before the change, you must reboot the AX device.

Example The following command globally changes the default number of retries to 5:

```
AX(config)#health global retry 5
```

Example The following command globally changes the timeout to 10 seconds and default number of retries to 4:

```
AX(config)#health global timeout 10 retry 4
```

health monitor

Description Configure a health monitor.

Syntax

```
[no] health monitor monitor-name
[interval seconds]
[retry number]
[timeout seconds]
[up-retry number]
```

Parameter	Description
monitor-name	Name of the health monitor, 1-31 characters.
interval *seconds*	Number of seconds between health check attempt, 1-180 seconds. A health check attempt consists of the AX 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. Default is 5 seconds.
retry *number*	Maximum number of times the AX Series will send the same health check to an unresponsive server before determining that the server is down. You can specify 1-5. Default is 3.
timeout *seconds*	Number of seconds the AX Series waits for a reply to a health check, 1-12 seconds. Default is 5 seconds.
up-retry *number*	Number of consecutive times the device must pass the same periodic health check, in order to be marked Up. You can specify 1-10. The default is 1.

Note: The **timeout** parameter is not applicable to external health monitors.

Default See above.

Mode Configuration mode

Usage For information about the commands available at the health-monitor configuration level, see "Config Commands: Health Monitors" on page 663.

Example The following command creates a health monitor named "hm1" and accesses the configuration level for it:

```
AX(config)#health monitor hm1
AX(config-health:monitor)#
```

health postfile

Description Import or delete a POST data file for an HTTP or HTTPS health check.

Syntax **health postfile {import | delete}** *filename*

Parameter	Description
import | delete	Specifies whether you are importing a POST data file or deleting one.
filename	Specifies the filename.

Default N/A

Mode Configuration mode

Usage

The maximum length of POST data you can specify in the CLI or GUI is 255 bytes. For longer data (up to 2 Kbytes), you must import the data in a file and refer to the file in the HTTP or HTTPS health check.

To use a POST data payload file in an HTTP/HTTPS health monitor, use the **postfile** *filename* option in the **method http** or **method https** command, at the configuration level for the health monitor.

Example

The following commands import a file containing a large HTTP POST data payload (up to 2 Kbytes), and add the payload to an HTTP health monitor:

```
AX(config)#health postfile import long-post
AX(config)#health monitor http1
AX2000(config-health:monitor)#method http url post / postfile long-post expect
def
```

In this example, health checks that use this health monitor will send a POST request containing the data in “postfile”, and expect the string “def” in response.

hostname

Set the AX Series device’s hostname.

Syntax Description

`[no] hostname string`

Parameter	Description
string	String of 1-31 characters.

Default

AX

Mode

Configuration mode

Usage

The CLI command prompt also is changed to show the new hostname.

Example

The following example sets the hostname to “SLBswitch2”:

```
AX(config)#hostname SLBswitch2
```

icmp-rate-limit

Description

Configure ICMP rate limiting, to protect against denial-of-service (DoS) attacks.

Syntax

```
[no] icmp-rate-limit normal-rate lockup max-rate
lockup-time
```

Parameter	Description
normal-rate	Maximum number of ICMP packets allowed per second. If the AX 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.
lockup *max-rate*	Maximum number of ICMP packets allowed per second before the AX device locks up ICMP traffic. When ICMP traffic is locked up, all ICMP packets are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the AX 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 AX device. To configure ICMP rate limiting on individual Ethernet interfaces, see “icmp-rate-limit” on page 209. To configure it in a virtual server template, see “slb template virtual-server” on page 640. 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:

```
AX(config)#icmp-rate-limit 2048 lockup 3000 10
```

interface

Description Access the CLI configuration level for an interface.

Syntax

```
interface {ethernet port-num | ve ve-num |
loopback num | management | trunk num}
```

Default N/A

Mode Configuration mode

Usage For information about the commands available at the interface configuration level, see “Config Commands: Interface” on page 203.

Example The following command changes the CLI to the configuration level for Ethernet interface 3:

```
AX(config)#interface ethernet 3
AX(config-if:ethernet3)#
```

ip

Description Configure global IP settings. For information, see “Config Commands: IP” on page 239.

ip-list

Description Configure a list of client addresses. IP lists can be used with features such as Fixed-NAT and client mobile number logging.

Syntax

```
[no] ip-list list-name
```

This command changes the CLI to the configuration level for the specified IP list, where the following command is available.

Command	Description
`[no] start-ipv4-addr to end-ipv4-addr`	Range of IPv4 addresses. Enter the lowest address number in the range first.
`[no] start-ipv6-addr to end-ipv6-addr`	Range of IPv6 addresses. Enter the lowest address number in the range first.

Default None

Mode Configuration mode

Usage See the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.

Introduced in Release 2.6.6-P4

ipv6

Description Configure global IPv6 settings. For information, see "Config Commands: IPv6" on page 265.

key chain

Configure a key chain for use by RIP or IS-IS MD5 authentication.

Syntax Description

```
[no] key chain name
```

Parameter	Description
name	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:

Command	Description
`[no] key num`	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`* – 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, A10 Networks recommends using one key chain per interface, per routing protocol.

Example The following commands configure a key chain named “example_chain”.

```
AX(config)#key chain example_chain
AX(config-keychain)#key 1
AX(config-keychain-key)#key-string thisiskey1
AX(config-keychain-key)#exit
AX(config-keychain)#key 2
AX(config-keychain-key)#key-string thisiskey2
AX(config-keychain-key)#exit
AX(config-keychain)#key 3
AX(config-keychain-key)#key-string thisiskey3
```

l3-vlan-fwd-disable

Description Globally disable Layer 3 forwarding between VLANs.

Syntax `[no] l3-vlan-fwd-disable`

Default By default, the AX device can forward Layer 3 traffic between VLANs.

Mode Configuration mode

Usage This option is applicable only on AX devices deployed in gateway (route) mode. If the option to disable Layer 3 forwarding between VLANs is configured at any level, the AX 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. (See“l3-vlan-fwd-disable” on page 226.)

- Access Control Lists (ACLs) – Layer 3 forwarding between VLANs is disabled for all traffic that matches ACL rules that use the **l3-vlan-fwd-disable** action. (See “access-list (standard)” on page 80 or “access-list (extended)” on page 82.)

To display statistics for this option, see “show slb switch” on page 772.

lacp system-priority

Description Set the Link Aggregation Control Protocol (LACP) priority.

Syntax

```
[no] lacp system-priority num
```

Parameter	Description
num	Specifies 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 AX 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-trunk

Description Configure settings for an LACP trunk.

Syntax

```
[no] lacp-trunk Trunknum
```

Parameter	Description
Trunknum	Specifies the LACP trunk ID.

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

Command	Description
disable-lacp [ethernet *portnum*	

[**to** *portnum*] [**ethernet** *portnum* ...]]	Disables the trunk or specific interfaces in the trunk.
enable-lacp [**ethernet** *portnum* [**to** *portnum*] [**ethernet** *portnum* ...]]	Enables the trunk or specific interfaces in the trunk.
[**no**] **ports-threshold** *num* [**do-manual-recovery**]	Specifies the 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 AX automatically disables the trunk's member ports. The ports are disabled in the running-config. You can specify 2-8. The **do-manual-recovery** option disables automatic recovery of the trunk when the required number of ports come back up. If you use this option, the trunk remains disabled until you re-enable it.
[**no**] **ports-threshold-timer** *seconds*	Specifies how many seconds to wait after a port goes down before marking the trunk down, if the configured threshold is exceeded. You can set the ports-threshold timer to 1-300 seconds.

Default

The global LACP trunk parameters have the following default settings:

- **disable-lacp** / **enable-lacp** – Enabled
- **ports-threshold** – Not set. By default, a trunk's status remains Up so long as at least one of its member ports is up
- **ports-threshold-timer** – 10 seconds

Mode

Configuration mode

Usage

Notes Regarding the Ports Threshold

If the number of up ports falls below the configured threshold, the AX automatically disables the trunk's member ports. The ports are disabled in the running-config. The AX device also generates a log message and an SNMP trap, if these services are enabled.

In some situations, a timer is used to delay the ports-threshold action. The configured port threshold is not enforced until the timer expires. The ports-threshold timer for a trunk is used in the following situations:

- When a member of the trunk links up.
- A port is added to or removed from the trunk.
- The port threshold for the trunk is configured during runtime. (If the threshold is set in the startup-config, the timer is not used.)

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 AX device most recently rebooted.

Syntax

```
link startup-config {default | profile-name}
[primary | secondary] [cf]
```

Parameter	Description
default	Links “startup-config” to the configuration profile stored in the image area from which the AX device was most recently rebooted.
profile-name	Links “startup-config” to the specified configuration profile.
primary | secondary	Specifies the image area. If you omit this option, the image area last used to boot is selected.
cf	Links the profile to the specified image area in compact flash instead of the hard disk.

Default

The “startup-config” token is linked to the configuration profile stored in the image area from which the AX 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 all** and **show startup-config all cf** commands. See “show startup-config” on page 778.)

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 AX 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”:

```
AX(config)#link startup-config slbconfig3
```

Example The following command relinks “startup-config” to the configuration profile stored in the image area from which the AX device was most recently rebooted”:

```
AX(config)#link startup-config default
```

locale

Set the CLI locale.

Syntax Description

```
[no] locale {test | locale}
```

Default en_US.UTF-8

Mode Configuration mode

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

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

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

logging auditlog host

Description

Configure audit logging to an external server.

Syntax

```
[no] logging auditlog host {ipaddr | hostname}
[facility facility-name]
```

Parameter	Description
ipaddr | hostname	IP address or hostname of the server.
facility-name	Name of a log facility: **local0** **local1** **local2** **local3** **local4** **local5** **local6** **local7** There is no default.

Default

Not set

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. To back up the system log, see “backup log” on page 59 or “backup periodically” on page 99.

In the current release, only a single log server is supported for remote audit logging.

logging *target severity-level*

Description

Specify the severity levels of event messages to send to message targets other than the AX log buffer.

Syntax

```
[no] logging target severity-level
```

Parameter	Description
target	Specifies where event messages are sent: **console** – serial console **email** – email **monitor** – Telnet and SSH sessions **syslog** – external Syslog host **trap** – external SNMP trap host

Note: For information about the email option, see "logging email buffer" on page 141. and "logging email filter" on page 142.

Parameter	Description

severity-level	Specifies the severity levels to log. You can enter the name or the number of the severity level.
	{**0** | **emergency**}
	{**1** | **alert**}
	{**2** | **critical**}
	{**3** | **error**}
	{**4** | **warning**}
	{**5** | **notification**}
	{**6** | **information**}
	{**7** | **debugging**}

Default

The default severity level depends on the target:

- **console** – 3 (error)
- **email** – not set (no logging)
- **monitor** – not set (no logging)
- **syslog** – not set (no logging)
- **trap** – not set (no logging)

Mode

Configuration mode

Usage

To send log messages to an external host, you must configure the external host using the **logging host** command.

Example

The following command sets the severity level for event messages sent to the console to 2 (critical):

```
AX(config)#logging console 2
```

logging buffered

Description Configure the event log on the AX Series device.

Syntax

```
[no] logging buffered
{maximum-messages | severity-level}
```

Parameter	Description
maximum-messages	Specifies the maximum number of messages the event log buffer will hold.

severity-level	Specifies the severity levels to log. You can enter the name or the number of the severity level.
	{**0**|**emergency**}
	{**1**|**alert**}
	{**2**|**critical**}
	{**3**|**error**}
	{**4**|**warning**}
	{**5**|**notification**}
	{**6**|**information**}
	{**7**|**debugging**}

Default The default buffer size (maximum messages) is 30000. The default severity level is 7 (debugging).

Mode Configuration mode

Example The following command sets the severity level for log messages to 7 (debugging):

```
AX(config)#logging buffered 7
```

logging email buffer

Description Configure log email settings.

Syntax

```
[no] logging email buffer [number num]
[time minutes]
```

Parameter	Description
number *num*	Specifies the maximum number of messages to buffer. You can specify 16-256.
time *minutes*	Specifies how long to wait before sending all buffered messages, if the buffer contains fewer than the maximum allowed number of messages. You can specify 10-1440 minutes.

Default

By default, emailing of log messages is disabled. When you enable the feature, the buffer options have the following default values:

- **number** – 50
- **time** – 10

Mode

Configuration mode

Usage

To configure the AX 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. See "logging email filter" on page 142 and "logging email-address" on page 144.

Example

The following command configures the AX 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.

```
AX(config)#logging email buffer number 32 time 30
```

logging email filter

Description

Configure a filter for emailing log messages.

Syntax

```
[no] logging email filter filter-num
conditions operators
[trigger]
```

Parameter	Description
filter-num	Specifies the filter number, 1-8.
conditions	Message attributes on which to match. The conditions list can contain one or more of the following: **level** *severity-levels* – Specifies the severity levels of messages to send in email. You can specify the severity levels by number (0-7) or by name:

emergency, **alert**, **critical**, **error**, **warning**, **notification**, **information**, or **debugging**.

mod *software-module-name* – Specifies the 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.

pattern *regex* – Specifies the string requirements. Standard regular expression syntax is supported. Only messages that meet the criteria of the regular expression will be emailed. The regular expression can be a simple text string or a more complex expression using standard regular expression logic.

operators

Set of Boolean operators (AND, OR, NOT) that specify how the conditions should be compared.

The CLI Boolean expression syntax is based on Reverse Polish Notation (also called Postfix Notation), a notation method that places an operator (AND, OR, NOT) after all of its operands (in this case, the conditions list).

After listing all the conditions, specify the Boolean operator(s). The following operators are supported:

AND – All conditions must match in order for a log message to be emailed.

OR – Any one or more of the conditions must match in order for a log message to be emailed.

NOT – A log message is emailed only if it does not match the conditions

(For more information about Reverse Polish Notation, see the following link: http://en.wikipedia.org/wiki/Reverse_Polish_notation.)

trigger

Immediately sends the matching messages in an email instead of buffering them. If you omit this option, the messages are buffered based on the **logging email buffer** settings.

Default

Not set. Emailing of log messages is disabled by default.

Mode

Configuration mode

Usage

To configure the AX device to send log messages by email, you also must specify the email address to which to email the log messages. See "logging email-address" on page 144.

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.
- For backward compatibility, the following syntax from previous releases is still supported:

  logging email *severity-level*

  The *severity-level* can be one or more of the following: **0**, **1**, **2**, **5**, **emergency**, **alert**, **critical**, **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.

```
AX(config)#logging email filter 1 level information pattern "abc" and
```

Example

The following command reconfigures the filter to immediately email matching messages.

```
AX(config)#logging email filter 1 level information pattern "abc" and trigger
```

logging email-address

Description

Specify the email addresses to which to send event messages.

Syntax

```
[no] logging email-address address [...]
```

Parameter	Description
address	Specifies an email address. You can enter more than one address on the command line. Use a space between each address.

Default None

Mode Configuration mode

Usage To configure the AX device to send log messages by email, you also must configure an email filter. See "logging email filter" on page 142.

Example The following command sets two email addresses to which to send log messages:

```
AX(config)#logging email-address admin1@example.com admin2@example.com
```

logging export

Description Send the messages that are in the event buffer to an external file server.

Syntax `[no] logging export [all] url`

Parameter	Description
all	Include system support messages.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp**://*host*/*file* **ftp**://[*user*@]*host*[:*port*]/*file* **scp**://[*user*@]*host*/*file* **rcp**://[*user*@]*host*/*file*

Default N/A

Mode Configuration mode

logging facility

Description Enable logging facilities.

Syntax

```
[no] logging facility facility-name
```

Parameter	Description
facility-name	Name of a log facility: **local0** **local1** **local2** **local3** **local4** **local5** **local6** **local7**

Default The default facility is local0.

Mode Configuration mode

logging host

Description Specify a Syslog server to which to send event messages.

Syntax

```
[no] logging host ipaddr [ipaddr...]
[port protocol-port]
```

Parameter	Description
ipaddr	IP address of the Syslog server. You can enter multiple IP addresses. Up to 10 remote logging servers are supported.
port *protocol-port*	Protocol port number to which to send messages. You can specify only one protocol port with the command. All servers must use the same protocol port to listen for syslog messages.

Default The default protocol port is 514.

Mode Configuration mode

Usage If you use the command to add some log servers, then need to add a new log server later, you must enter all server IP addresses in the new command. Each time you enter the **logging host** command, it replaces any set of servers and syslog port configured by the previous **logging host** command.

Example The following command configures 4 external log servers. In this example, the servers use the default syslog protocol port, 514, to listen for log messages.

```
AX(config)#logging host 1.1.1.1 2.2.2.2 3.3.3.3 4.4.4.4
```

Example The following command reconfigures the set of external log servers, with a different protocol port. All the log servers must use this port.

```
AX(config)#logging host 1.1.1.1 2.2.2.2 3.3.3.3 4.4.4.4 port 8899
```

lsn-lid

Description Configure a limit ID (LID) for LSN. See “lsn-lid” on page 479.

lsn-rule-list

Description Configure a rule list for LSN. See “lsn-rule-list” on page 482.

lw-4o6

Description Configure Lightweight 4over6. See “Config Commands: Lightweight 4over6” on page 569.

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
mac-address	Hardware address, in the following format: *aabb***.***ccdd***.***eeff*

port *port-num*	AX Ethernet port to which to assign the MAC address.
vlan *vlan-id*	Layer 2 broadcast domain in which to place the device.
trap	Send packets to the CPU for processing, instead of switching them in hardware. **source** – Send packets that have this MAC as a source address to the CPU. **dest** – Send packets that have this MAC as a destination address to the CPU. **both** – Send packets that have this MAC as either a source or destination address to the CPU.

Note: The **trap** option is supported only on models AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200. On models AX 5100 and AX 5200, only **trap dest** is supported.

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:

```
AX(config)#mac-address abab.cdcd.efef port 5 vlan 3
```

mac-age-time

Description Set the aging time for dynamic (learned) MAC entries. An entry that remains unused for the duration of the aging time is removed from the MAC table.

Syntax **[no] mac-age-time** *seconds*

Parameter	Description
seconds	Number of seconds a learned MAC entry can remain unused before it is removed from the MAC table. You can specify 10-600 seconds.

Default 300 seconds

Mode Configuration mode

Usage On models AX 1000, AX 2000, AX 2100, and AX 3000, the actual MAC aging time can be +/- 10 seconds from the configured value.

On models AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200, 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.

Example The following command changes the MAC aging time to 600 seconds:

```
AX(config)#mac-age-time 600
```

maximum-paths

Description Change the maximum number of paths a route can have in the forwarding Information Base (FIB).

Syntax `[no] maximum-paths num`

Parameter	Description
num	Maximum number of paths a route can have. You can specify 1-10.

Default 4

Mode Configuration mode

mirror-port

Description Specify a port to which to copy monitored traffic to or from another port.

Syntax `[no] mirror-port ethernet port-num`

Parameter	Description
port-num	Ethernet port number out which the monitored traffic will be sent.

Default No ports are mirrored.

Mode Configuration mode

Usage To specify the port to monitor, use the **monitor** command at the interface configuration level. (See "monitor" on page 230.)

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:

```
AX(config)#mirror-port ethernet 3
AX(config)#interface ethernet 5
AX(config-if:ethernet5)#monitor input
```

monitor

Description Specify event thresholds for utilization of resources.

Syntax

```
monitor {buffer-drop | buffer-usage | ctrl-cpu |
data-cpu | disk | memory | warn-temp}
threshold-value
```

Parameter	Description
buffer-drop	Packet drops (dropped IO buffers)
buffer-usage	Control buffer utilization
ctrl-cpu	Control CPU utilization
data-cpu	Data CPUs utilization
disk	Hard disk utilization
memory	Memory utilization
warn-temp	CPU temperature
threshold-value	The values you can specify depend on the event type and on the AX model. For information, see the CLI help.

Default The default threshold values depend on the event type and on the AX model. For information, see the CLI help.

Usage If utilization of a system resource crosses the configured threshold, a log message is generated. If applicable, an SNMP trap is also generated.

To display the configured event thresholds, see "show monitor" on page 753.

Example The following command sets the event threshold for data CPU utilization to 80%:

```
AX(config)#monitor data-cpu 80
```

multi-config

Description Configure multiple simultaneous administrative sessions.

Syntax

```
[no] multi-config enable
```

Default Disabled

Mode Configuration mode

Usage Previous releases allowed only a single admin to access the AX device in configuration mode. However, the AX device now supports multiple, simultaneous configuration sessions. When the **multi-config** feature is enabled, configuration commands across all admins sessions will apply immediately to the AX device, without terminating another admin's session.

Enabling Multi-User Access

When an additional user attempts to access the device in configuration mode, the original admin is prompted to permit access. If permission is granted, multiple admins may freely access the device without the display of subsequent prompts.

Disabling Multi-User Access

Disabling multiple admin access does not terminate currently active admin sessions. For example, if 4 admin accounts are simultaneously accessing the device in configuration mode, disabling multi-user access will deny access when a 5th user attempts to log onto the device. However, the previous 4 admin sessions will continue to run unaffected.

Simultaneous Parameter Configuration

Multiple admins may configure the same parameter in real-time. When two admins modify the same configuration option, the most recent changes are applied.

If a parameter is undergoing configuration and a second admin attempts to disable or delete the parameter, the AX device will warn the second admin that the item is currently in use.

If an admin disables an option and a second admin attempts to configure the same option, the AX device will return a message that the option does not exist.

Reloading the AX Device

You can reload the AX device only when there is a single admin session in configuration mode. If you attempt to reload the AX device while multiple configuration sessions are running, an warning notification appears.

To reload the AX device when there are multiple configuration sessions, use the command **clear admin sessions** from the global configuration level of the CLI. After clearing all admin sessions, reload the AX device, and additional admins can immediately re-log onto the device.

nat46-stateless

Description

Configure stateless NAT46. See "Config Commands: Stateless NAT46" on page 577.

nat64

Description

Configure global settings for NAT64. See "Config Commands: NAT64 / DNS64" on page 513.

netflow

Description

Enable the AX 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
```

Parameter	Description
monitor-name	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
destination {service-group *sg-name* | *ip-addr*}	Configure the destination where NetFlow records will be sent by entering a service group (if using

multiple NetFlow collectors), or an IP address for a specific host.

`disable`

Disable this NetFlow monitor.

`enable`

Enable this NetFlow monitor.

`flow-timeout`

Timeout value interval at which flow records will be periodically exported for long-lived sessions. Flow records for short-lived sessions (if any) are sent upon termination of the session.

After the specified amount of time has elapsed, the AX 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.

Setting the timeout value to 0 disables the flow timeout feature. Regardless of how long-lived a flow might be, the AX device waits until the flow has ended and the session is deleted before it sends any flow records for it.

`monitor {ethernet | global | nat-pool}`

Configure filters for monitoring traffic. Identify the specific type and subset of resources to monitor. You can specify monitoring of one or the other of the following resources:

ethernet – Specify the list of ports to monitor. Flow information for the monitored interfaces is sent to the NetFlow collector(s).

global – (Default) No filters are in effect. Traffic on all interfaces and for all NAT pools is monitored.

nat-pools – Specify the pool of NAT addresses to monitor. Flow information for the monitored IP addresses is sent to the NetFlow collector(s). Currently, only CGN pools can be entered; standard (non-CGN pools) are not supported.

`protocol`

Configure which version of the NetFlow protocol to use, version 9 or version 10. The default is NetFlow version 9.

`[no]` **`record`** *`netflow-template-type`*

[both | creation | deletion]

Configure the NetFlow record types to be exported. (See the "NetFlow v9 and v10 (IPFIX)" chapter in the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.)

The *netflow-template-type* refers to the NetFlow template that defines the NetFlow records to export, and it includes the following template types:

- **nat44**
- **nat64**
- **dslite**
- **sesn-event-nat44**
- **sesn-event-nat64**
- **sesn-event-dslite**
- **port-mapping-nat44**
- **port-mapping-nat64**
- **port-mapping-dslite**

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.

resend-template {records *num* **|**

timeout *seconds*}

Configure when to resend the NetFlow template. The trigger can be either the number of records, or the amount of time that has passed.

records – 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.

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 AX port from which NetFlow traffic is exported.

Default

Described above, where applicable.

Introduced in Release

2.6.6-P4

Mode

Configuration mode

Usage

A NetFlow monitor consists of the following protocol parameters, which can be used to configure the AX 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.

Predefined NetFlow Templates

The AX device includes some pre-defined NetFlow templates. For information, see the “NetFlow v9 and v10 (IPFIX)” chapter in the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.

no

Description

Remove a configuration command from the running configuration.

Syntax

no *command-string*

Default

N/A

Mode

Config

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. (See "write" on page 201.)

Example The following command removes server "http99" from the running-config:

```
AX(config)#no slb server http99
```

ntp

Description Configure Network Time Protocol (NTP) parameters.

Syntax

```
[no] ntp server {hostname | ipaddr}
```

```
[no] ntp {disable | enable}
```

Parameter	Description
hostname | *ipaddr*	Hostname or IP address of the NTP server.
disable	Disables synchronization with the NTP server.
enable	Enables synchronization with the NTP server.

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:

```
AX(config)#ntp server 10.1.4.20
AX(config)#ntp server enable
```

ping

Ping is used to diagnose basic network connectivity. For syntax information, see “ping” on page 53.

radius-server

Description

Set RADIUS parameters, for authenticating administrative access to the AX Series device.

Syntax

```
[no] radius-server host {hostname | ipaddr}
       secret secret-string
       [acct-port protocol-port]
       [auth-port protocol-port]
       [retransmit num]
       [timeout seconds]
       [default-privilege-read-write]
```

Parameter	Description
hostname | *ipaddr*	Hostname or IP address of the RADIUS server.
secret *secret-string*	Password, 1-128 characters, required by the RADIUS server for authentication requests.
acct-port *protocol-port*	Protocol port to which the AX Series device sends RADIUS accounting information.
auth-port *protocol-port*	Protocol port to which the AX Series device sends authentication requests.
retransmit *num*	Maximum number of times the AX device can resend an unanswered authentication request to the server. If the AX device does not receive a reply to the final request, the AX device tries the secondary server, if one is configured. If no secondary server is available, or if the secondary server also fails to reply after the maximum number of retries, authentication fails and the admin is denied access. You can specify 0-5 retries.

timeout *seconds*	Maximum number of seconds the AX device will wait for a reply to an authentication request before resending the request. You can specify 1-15 seconds.
default-privilege-read-write	Change the default privilege authorized by RADIUS from read-only to read-write. The default privilege is used if the Service-Type attribute is not used, or the A10 vendor attribute is not used.

Default

No RADIUS servers are configured by default. When you add a RADIUS server, it has the following default settings:

- **acct-port** – 1813
- **auth-port** – 1812
- **retransmit** – 3 retries
- **timeout** – 3 seconds
- **default-privilege-read-write** – 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.

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 AX 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.

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

raid

Description Enter the configuration level for RAID.

Syntax

```
raid
```

CAUTION! RAID configuration should be performed only by or with the assistance of A10 Networks. A10 strongly advises that you do not experiment with these commands.

restore

Description Restore the startup-config and SSL certificates and keys from a tar file previously created by the **backup** command. The restored configuration takes effect following a reboot.

Syntax

```
restore [use-mgmt-port] url
```

Parameter	Description
`use-mgmt-port`	Uses the management interface as the source interface for the connection to the remote device. The management route table is used to reach the device. By default, the AX device attempts to use the data route table to reach the remote device through a data interface.
`url`	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long. To enter the entire URL: **tftp:**//*host*/*file* **ftp:**//[*user*@]*host*[:*port*]/*file* **scp:**//[*user*@]*host*/*file* **rcp:**//[*user*@]*host*/*file*

Default N/A

Mode

Configuration mode

Usage

Do not save the configuration (**write memory**) after restoring the startup-config. If you do, the startup-config will be replaced by the running-config and you will need to restore the startup-config again.

To place the restored configuration into effect, reboot the AX device.

The “**no**” form of this command is invalid.

route-map

Description

Configure a rule in a route map. You can use route maps to provide input to the following OSPF commands:

- “redistribute” on page 321
- “default-information originate” on page 331

Syntax

```
[no] route-map map-name {deny | permit}
sequence-num
```

Parameter	Description
map-name	Route map name.
deny | permit	Action to perform on data that matches the rule.
sequence-num	Sequence number of the rule within the route map, 1-65535. Rules are used in ascending sequence order. The action in the first matching rule is used, and no further matching is performed. You do not need to configure route map rules in numerical order. The CLI automatically places them in the configuration (running-config) in ascending numerical order.

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

Note: Some match options apply only to BGP, which is not supported in the current release.

Command	Description
match as-path *acl-id*	Matches on the BGP AS paths listed in the specified ACL.
match community *acl-id* [**exact-match**]	Matches on the BGP communities listed in the specified ACL.
match extcommunity *acl-id* [**exact-match**]	Matches on the BGP external communities listed in the specified ACL.
match interface {**ethernet** *portnum* | **loopback** *num* | **management** | **ve** *ve-num*}	Matches on the interface used as the first hop for a route.
match ip address {*acl-id* | **prefix-list** *list-name*}	Matches on the route IP addresses in the specified ACL or prefix list.
match ip next-hop {*acl-id* | **prefix-list** *list-name*}	Matches on the next-hop router IP addresses in the specified ACL or prefix list.
match ip peer *acl-id*	Matches on the peer router IP addresses in the specified ACL.
match ipv6 address {*acl-id* | **prefix-list** *list-name*}	Matches on the route IP addresses in the specified ACL or prefix list.

match ipv6 next-hop {*acl-id* | **prefix-list** *list-name* | *ipv6-addr*} — Matches on the next-hop router IP addresses in the specified ACL or prefix list, or the specified IPv6 address.

match ipv6 peer *acl-id* — Matches on the peer router IP addresses in the specified ACL.

match metric *num* — Matches on the specified metric value, 0-4294967295.

match origin {**egp** | **igp** | **incomplete**} — Matches on the specified BGP origin code.

match route-type external {**type-1** | **type-2**} — Matches on the specified external route type.

match tag — Matches on the specified TAG value, 0-4294967295.

Default None

Mode Configuration mode

Usage For options that use an ACL, the ACL must use a permit action. Otherwise, the route map action is deny.

router *protocol*

Description Enter the configuration mode for a dynamic routing protocol.

Syntax

```
[no] router protocol
```

Parameter	Description
protocol	Specifies the routing protocol: **bgp** *AS-num* – Specifies an Autonomous System (AS) for which to run BGP on the AX device. **ipv6 ospf** [*tag*] – Specifies an IPv6 OSPFv3 process (1-65535) to run on the IPv6 link. **ipv6 rip** – Enables IPv6 RIP. **isis** [*tag*] – Enables Intermediate System to Intermediate System (IS-IS). **log** – See the following sections: "router log file" on page 164 "router log record-priority" on page 165 "router log stdout" on page 165 "router log trap" on page 166 **ospf** [*process-id*] – Specifies an IPv4 OSPFv2 process (1-65535) to run on the AX device. **rip** – Enables IPv4 RIP.

Note: After you enter the command, the CLI changes to the configuration level for the specified protocol.

Default Dynamic routing protocols are disabled by default.

Mode Configuration mode

Usage This command is valid only when the AX is configured for gateway mode (Layer 3).

For more information, see the following:

- "Config Commands: Router – RIP" on page 279
- "Config Commands: Router – OSPF" on page 311

- “Config Commands: Router – IS-IS” on page 359
- “Config Commands: Router – BGP” on page 395

Example

The following command enters the configuration level for OSPFv2 process 1:

```
AX(config)#router ospf 1
AX(config-router)#
```

router log file

Description

Configure router logging to a local file.

Syntax

```
[no] router log file
{
name string |
per-protocol |
rotate num |
size Mbytes
}
```

Parameter	Description
name *string*	Name of the log file.
per-protocol	Uses separate log files for each protocol. Without this option, log messages for all protocols are written to the same file.
rotate *num*	Specifies the number of backups to allow for each log file. When a log file becomes full, the logs are saved to a backup file and the log file is cleared for new logs. You can specify 0-100 backups. Older backups are purged to make way for new ones if the maximum number is reached.
size *Mbytes*	Specifies the size of each log file. You can specify 0-1000000 Mbytes. If you specify 0, the file size is unlimited.

Default

This command has the following default values:

- **per-protocol** – disabled
- **rotate** – 0
- **size** – 0 (unlimited)

Mode

Configuration mode

Usage When you enable logging, the default minimum severity level that is logged is debugging. To change the minimum severity level that is logged, see "router log trap" on page 166.

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 Enable router logging to the local log buffer.

Syntax

```
[no] router log log-buffer
```

Default Disabled

Mode Configuration mode

router log record-priority

Description Include the message priority within each router log message.

Syntax

```
[no] router log record-priority
```

Default Disabled

Mode Configuration mode

router log stdout

Description Enable router logging to the terminal.

Syntax

```
[no] router log stdout
```

Default Disabled

Mode Configuration mode

Usage When you enable logging, the default minimum severity level that is logged is debugging. To change the minimum severity level that is logged, see "router log trap" on page 166.

router log trap

Description

Specify the minimum severity level to log for router logs.

Syntax

```
[no] router log trap severity-level
```

Parameter	Description
severity-level	Minimum severity level to log. You can specify one of the following: **emergencies** **alerts** **critical** **errors** **warnings** **notifications** **informational** **debugging**

Default

debugging

Mode

Configuration mode

run-hw-diag

Description

Access the hardware diagnostics menu.

Caution: **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:

```
AX(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.
AX(config)#end
AX#reboot
Proceed with reboot? [yes/no]:yes


Rebooting......

INIT: version 2.86 booting
Booting.........mdadm: stopped /dev/md1
mdadm: stopped /dev/md0

00000000000

------------------------------------------------------
|      Hardware Diagnostic Menu                      |
------------------------------------------------------
|  1 - Memory Test                                   |
|  2 - HDD/CF Scan Test (1-2 hours)                  |
|  3 - MBR (Master Boot Record) check                |
|  4 - Complete Test (all above)                     |
|  x - Reboot                                        |
------------------------------------------------------

Please select an option [1-4, x]:
```

session strict-aging-on-clear

Description

Please contact A10 Networks.

Syntax

```
[no] session strict-aging-on-clear
```

Default

Disabled

Mode

Configuration mode

session-filter

Description

Configure a session filter.

```
session-filter filter-name
{
6rd-nat64 sub-options |
ds-lite sub-options |
ipv4 sub-options |
ipv6 sub-options |
nat44 sub-options |
nat64 sub-options
}
```

Parameter	Description
6rd-nat64 *sub-options*	Matches on IPv6-in-IPv4 6rd-NAT64 sessions. The following *sub-options* are supported: **source-v4-addr** *ipv4addr*[*/mask-length*] – Source IPv4 address of the session. **source-v6-addr** *ipv6addr*[*/prefix*] – Source IPv6 address of the session. **source-port** *portnum* – Source protocol port of the session.

dest-v4-addr *ipv4addr*[*/mask-length*] – Destination IPv4 address of the session.

dest-v6-addr *ipv6addr*[*/prefix*] – Destination IPv6 address of the session.

dest-port *portnum* – Destination protocol port of the session.

ds-lite *sub-options*

Matches on IPv4-in-IPv6 DS-Lite sessions. The *sub-options* are the same as those for **6rd-nat64**.

ipv4 *sub-options*

Matches on IPv4 LSN sessions, IPv4 Fixed-NAT sessions, and IPv4 static mapping sessions. The following *sub-options* are supported:

source-v4-addr *ipv4addr*[*/mask-length*] – Source IPv4 address of the session.

source-port *portnum* – Source protocol port of the session.

dest-v4-addr *ipv4addr*[*/mask-length*] – Destination IPv4 address of the session.

dest-port *portnum* – Destination protocol port of the session.

ipv6 *sub-options*

Matches on NAT64 sessions and NAT64 Fixed-NAT sessions. The following *sub-options* are supported:

source-v6-addr *ipv6addr*[*/prefix*] – Source IPv6 address of the session.

source-port *portnum* – Source protocol port of the session.

dest-v6-addr *ipv6addr*[*/prefix*] – Destination IPv6 address of the session.

dest-port *portnum* – Destination protocol port of the session.

nat44 *sub-options*	Matches on IPv4 LSN sessions and IPv4 Fixed-NAT sessions. The *sub-options* are the same as those for **ipv4**.
nat64 *sub-options*	Matches on NAT64 sessions and NAT64 Fixed-NAT sessions. The *sub-options* are the same as those for **ipv6**.

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.

sflow

Description Enables the AX device to collect information about Ethernet data interfaces and send the data to an external sFlow collector (v5).

Syntax

```
[no] sflow
{
agent address ipaddr |
collector ipaddr [portnum] |
counter-polling-interval seconds |
packet-sampling-rate num |
polling sub-options |
sampling ethernet interface |
source-ip-use-mgmt
}
```

Parameter	Description
agent address *ipaddr*	Configure an sFlow agent. The *ipaddr* value can be any valid IPv4 or IPv6 address. By default, sFlow datagrams use the management IP of the AX device as the source address, but you can specify a different IP address, if desired. The information will appear in the Layer 4 informa-

tion section of the sFlow datagram, and it is not used to make routing decisions.

collector *ipaddr*

Configure up to four sFlow collectors. The IP address is that of the sFlow collector device. You can optionally specify the port number, with a range from 1-65535. The default port number is 6343.

counter-polling-interval *seconds*

Configure the sFlow counter polling interval. The **interval** *seconds* option specifies the frequency with which statistics for an interface are periodically sampled and sent to the sFlow collector. The default globally configured polling interval is 20 seconds, but the range can be configured to a value from 1-200 seconds.

packet-sampling-rate *num*

Configure sFlow default packet sampling rate. The *num* option specifies the value of *N*, where *N* is the value of the denominator in the ratio at which a single packet will be sampled from a denominator ranging from 10-1000000. The default is 1000, meaning one packet out of every 1000 will be sampled.

polling {**cpu-usage** | **ethernet** *interface* | **lsn-pool-usage**}

Configure sFlow counter polling on a specified interface.

CPU usage is included in the sFlow datagram by default.

You can specify an Ethernet interface from 1-12. There is no default.

LSN NAT pool usage is included in the sFlow datagram by default.

sampling ethernet *interface* — Configure sFlow sampling on a specified interface. You can specify interface 1-12. There is no default.

source-ip-use-mgmt — Enable use of the management interface's IP as the source address for outbound sFlow packets.

Default

Described above, where applicable.

Introduced in Release

2.6.6-P4

Mode

Configuration mode

Usage

Enable either or both of the following types of data collection, for individual Ethernet data ports:

- Packet flow sampling – The AX device 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 – The AX device 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

- sFlow data collection is supported only for individual Ethernet data ports. The feature is not supported for VEs, trunk interfaces, loopback interfaces, or the management interface.
- Sampling of CGN packets is performed only on pre-translation packets. The samples do not carry post-translation header information.
- 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

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:

```
AX(config)#sflow collector 192.168.100.3
AX(config)#sflow source-ip-use-mgmt
```

slb

Description

Configure server resources for external logging for IPv6 migration features. (See "Config Commands: Server Resource Commands" on page 617.)

smtp

Description

Configure a Simple Mail Transfer Protocol (SMTP) server to use for sending emails from the AX device.

Syntax

```
[no] smtp {hostname | ipaddr}
[mailfrom email-src-addr]
[needauthentication]
[port protocol-port]
[username string password string]
```

Parameter	Description
hostname | ipaddr	Specifies an SMTP server.
mailfrom *email-src-addr*	Specifies the email address to use as the sender (From) address.
needauthentication	Specifies that authentication is required.
port *protocol-port*	Specifies the protocol port on which the server listens for SMTP traffic.
username *string* **password** *string*	Specifies the username and password required for access. The password can be 1-31 characters long.

Default

No SMTP servers are configured by default. When you configure one, it has the following default settings:

- **port** – 25
- **needauthentication** – disabled
- **mailfrom** – not set

Mode Configuration mode

Example The following command configures the AX Series device to use SMTP server “ourmailsrvr”:

```
AX(config)#smtp ourmailsrvr
```

snmp-server community

Description Configure an SNMP community string.

Syntax

```
[no] snmp-server community
read ro-community-string
[oid oid-value]
[remote {hostname | ipaddr mask-length |
ipv6-addr/prefix-length}]
```

Parameter	Description
ro-community-string	The read-only community string.
oid *oid-value*	Object ID. This option restricts the objects that the AX Series device returns in response to GET requests. Values are returned only for the objects within or under the specified OID.
remote {*hostname* | *ipaddr mask-length* | *ipv6-addr/prefix-length*]}	Restricts SNMP access to a specific host or subnet. When you use this option, only the specified host or subnet can receive SNMP data from the AX Series device by sending a GET request to this community.

Default The configuration does not have any default SNMP communities. When you configure one, all OIDs are allowed by default and all remote hosts are allowed by default.

Mode Configuration mode

Usage All SNMP communities are read-only. Read-write communities are not supported. The OID for A10 Networks AX Series objects is 1.3.6.1.4.1.22610.

The “**no**” form removes the read-only community string.

Example The following commands enable SNMP, define community string “A10_AX”, and restrict access to hosts in subnet 10.10.20.x/24 and to AX MIB objects only:

```
AX(config)#snmp-server enable
AX(config)#snmp-server community read A10_AX oid AxMgmt remote 10.10.20.0 24
```

Example The following commands enable SNMP, define community string “A10_AX2”, and restrict access to hosts in IPv6 network a101::1111:

```
AX(config)#snmp-server enable
AX(config)#snmp-server community read A10_AX2 remote a101::1111
```

snmp-server contact

Description Configure SNMP contact information.

Syntax

```
[no] snmp-server contact contact-name
```

Parameter	Description
contact-name	The contact person’s name.

Default Empty string

Mode Configuration mode

Usage The “**no**” form removes the contact information.

Example The following command defines the contact person as “snmp-admin”:

```
AX(config)#snmp-server contact snmp-admin
```

snmp-server enable

Description Enable the AX Series device to accept SNMP MIB data queries and to send SNMP v1/v2c traps.

To use SNMP on the device, you must enter this command. Enter this command first, then enter the other **snmp-server** commands to further configure the feature.

Syntax

```
[no] snmp-server enable
     [
      traps [
             routing {isis | ospf} [trap-name] |
             snmp [trap-name] |
             ha [trap-name] |
             network [trap-name] |
             slb [trap-name] |
             lsn [trap-name] |
             system [trap-name]
             ]
      ]
```

Parameter	Description
`traps`	Specifies the traps to enable. You can enable all traps, all traps of a specific type, or individual traps. To enable all traps, specify **traps**, without any additional options. To enable all traps of a specific type, specify one of the following: **`traps routing`** – Enables the following traps: **`isis`** – Enables traps for Intermediate System To Intermediate System (IS-IS) routing. To list the individual traps you enable or disable, enter the following: **snmp-server enable traps routing isis ?** **`ospf`** – Enables traps for Open Shortest Path First (OSPF) routing. To list the individual traps you enable or disable, enter the following: **snmp-server enable traps routing ospf ?** **`traps snmp`** – Enables the following traps: **`linkdown`** – Indicates that an Ethernet interface has gone down. **`linkup`** – Indicates that an Ethernet interface has come up. **`traps ha`** – Enables the following traps: **`active`** – Indicates that the AX device is going from HA Standby mode to Active mode.

`standby` – Indicates that the AX device is going from HA Active mode to Standby mode.

`active-active` – Indicates that an Active-Active HA configuration has been enabled.

`traps network` – Enables the following trap:

`trunk-port-threshold` – Indicates that the trunk ports threshold feature has disabled trunk members because the number of up ports in the trunk has fallen below the configured threshold. (To configure the threshold, see "trunk" on page 195.)

`traps slb` – Enables the following traps:

`application-buffer-limit` – Indicates that the configured SLB application buffer threshold has been exceeded. (See "monitor" on page 150.)

`server-conn-limit` – Indicates that an SLB server has reached its configured connection limit.

`server-conn-resume` – Indicates that an SLB server has reached its configured connection-resume value.

`server-down` – Indicates that an SLB server has gone down.

`server-up` – Indicates that an SLB server has come up.

`service-conn-limit` – Indicates that an SLB service has reached its configured connection limit.

`service-conn-resume` – Indicates that an SLB service has reached its configured connection-resume value.

`service-down` – Indicates that an SLB service has gone down.

`service-up` – Indicates that an SLB service has come up.

`vip-connlimit` – Indicates that the connection limit configured on a virtual server has been exceeded.

vip-connratelimit – Indicates that the connection rate limit configured on a virtual server has been exceeded.

vip-port-connlimit – Indicates that the connection limit configured on a virtual port has been exceeded.

vip-port-connratelimit – Indicates that the connection rate limit configured on a virtual port has been exceeded.

vip-port-down – Indicates that an SLB virtual service port has gone down.

vip-port-up – Indicates that an SLB virtual service port has come up. An SLB virtual server's service port is up when at least one member (real server and real port) in the service group bound to the virtual port is up.

traps lsn – Enables the following traps:

per-ip-port-usage-threshold *num* – Indicates that an Large Scale NAT (LSN) global IP address has reached its configured port usage threshold. The *num* option specifies the threshold. When port utilization on any LSN NAT IP address reaches this value, a notification is triggered. You can specify 10000-64512. There is no default.

total-port-usage-threshold *num* – Indicates that the AX device has reached its configured system-wide port usage threshold for LSN global IP addresses. The *num* option specifies the threshold. When port utilization on any LSN NAT IP address reaches this value, a notification is triggered. You can specify 10000-655350000. There is no default.

traffic-exceeded – Indicates that an LSN IP address pool has reached its threshold of available addresses.

traps system – Enables the following traps:

control-cpu-high – Indicates that the control CPU utilization is higher than the configured threshold. (See "monitor" on page 150.)

data-cpu-high – Indicates that data CPU utilization is higher than the configured threshold. (See "monitor" on page 150.)

fan – Indicates that a system fan has failed. Contact A10 Networks.

high-disk-use – Indicates that hard disk usage on the AX device is higher than the configured threshold. (See "monitor" on page 150.)

high-memory-use – Indicates that the memory usage on the AX device is higher than the configured threshold. (See "monitor" on page 150.)

high-temp – Indicates that the temperature inside the AX chassis is higher than the configured threshold. (See "monitor" on page 150.)

packet-drop – Indicates that the number of dropped packets during the previous 10-second interval exceeded the configured threshold. (See "monitor" on page 150.)

power – Indicates that a power supply has failed. Contact A10 Networks.

pri-disk – Indicates that the primary Hard Disk has failed or the RAID system has failed. In dual-disk models, the primary Hard Disk is the one on the left, as you are facing the front of the AX chassis.

restart – Indicates that the AX device is going to reboot or reload.

sec-disk – Indicates that the secondary Hard Disk has failed or the RAID system has failed. The secondary Hard Disk is the one on the right, as you are facing the front of the AX chassis.

Note: This trap does not apply to the following models: AX 2500, AX 2600, AX 3000, AX 5100, or AX 5200.

shutdown – Indicates that the AX device has shut down.

start – Indicates that the AX device has started.

Note: If you enter the **snmp-server enable** command without a **trap** option, the SNMP service is enabled but no traps are enabled.

Default The SNMP service is disabled by default and all traps are disabled by default.

Mode Configuration mode

Usage The “**no**” form disables traps.

Example The following command enables all traps:

```
AX(config)#snmp-server enable traps
```

snmp-server group

Description Configure an SNMP group.

Syntax

```
[no] snmp-server group group-name {v1 | v2c | v3
{auth | noauth | priv}} read view-name
```

Parameter	Description
group-name	Specifies the name of the SNMP group.
v1	Uses the least secure of the security models.
v2c	Uses the second-least secure of the security models.
v3	Uses the most secure of the security models.
auth	Uses packet authentication but does not encrypt the packets. (This is the authNoPriv security level.)
noauth	Does not use any authentication of packets. (This is the noAuthNoPriv security level.)
priv	Uses packet authentication and encryption. (This is the authPriv security level.)
view-name	Specifies the name of a read-only view for accessing the MIB object values.

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”:

```
AX(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 trap-receiver
[version {v1 | v2c}]
community-string
[udp-port port-num]
```

Parameter	Description
trap-receiver	Hostname or IP address of the remote device to which traps will be sent.
version {**v1** | **v2c**}	SNMP version. If you omit this option, the trap receiver can use SNMP v1 or v2c.
community-string	Community string for the traps.
port-num	UDP port to which the AX Series device will send the traps.

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 2 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.

```
AX(config)#snmp-server host 100.10.10.12 public udp-port 166
```

snmp-server location

Description Configure SNMP location information.

Syntax

```
[no] snmp-server location location
```

Parameter	Description
location	The location of this AX device.

Default Empty string

Mode Configuration mode

Usage The “**no**” form removes the location information.

Example The following command configures the location as “A10-HQ”:

```
AX(config)#snmp-server location A10-HQ
```

snmp-server user

Description Configure SNMP user-based groups.

Syntax

```
[no] snmp-server user user-name group group-name
{v1 | v2 | v3 [auth {md5 | sha} password
[encrypted]]}
```

Parameter	Description
user-name	Specifies the SNMP user name.
group-name	Specifies the group to which the SNMP user belongs.
v1 | **v2c**	Specifies SNMP version 1 or v2c.
v3 [**auth** {**md5** | **sha**} *password* [**encrypted**]]	Specifies SNMP version 3 and the authentication to use. **md5** | **sha** – HMAC MD5 (**md5**) or HMAC SHA (**sha**). *password* [**encrypted**] – Password, 8-31 characters, for SNMP messages. To encrypt the password, use the **encrypted** option.

Default No SNMP users are configured by default. When you configure one, all remote hosts are allowed by default. For v3, there is no authentication by default.

Mode Configuration mode

Example The following command adds an SNMP user belonging to group “group1”. The SNMP version is 3 and the authentication method is HMAC MD5. The password is “12345678”. The password is not encrypted.

```
AX(config)#snmp-server user user1 group group1 v3 auth md5 12345678
```

snmp-server view

Description Configure an SNMP view.

Syntax

```
[no] snmp-server view view-name oid [oid-mask]
{included | excluded}
```

Parameter	Description
view-name	SNMP views name.
oid	MIB view family name or OID.
oid-mask	OID mask. Use hex octets, separated by ‘.’.
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 A10 Networks AX Series objects 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:

```
AX(config)#snmp-server view view1 1.3.6 included
```

stats-data-disable

Description Globally disable collection of statistical data.

Syntax

```
stats-data-disable
```

Default Statistical data collection is enabled by default.

Mode Configuration mode

Usage This command disables statistical data collection for system resources, including the following:

- CPU
- Memory
- Disk
- Interfaces

This command also disables statistical data collection for any of the following types of load-balancing resources, if collection is enabled on those resources:

- SLB resources:
  - Real server
  - Real server port
  - Service group
  - Virtual server
  - Virtual server port

stats-data-enable

Description

Globally re-enable collection of statistical data.

Syntax

```
stats-data-enable
```

Default

Statistical data collection is enabled by default.

Mode

Configuration mode

Usage

This command re-enables statistical data collection for system resources, including the following:

- CPU
- Memory
- Disk
- Interfaces

The command also re-enables statistical data collection for any individual load-balancing resources on which collection had been enabled before it was globally disabled.

system {all-vlan-limit | per-vlan-limit}

Description

Set traffic limits for VLANs. You can set a global limit for all VLANs or per VLAN.

Syntax

```
[no] system {all-vlan-limit | per-vlan-limit}
{bcast | ipmcast | mcast | unknown_ucast} num
```

Parameter	Description
all-vlan-limit | per-vlan-limit	Specifies whether the limit is system-wide for all VLANs or for each individual VLAN. **all-vlan-limit** – Limit applies system-wide to all VLANs. Collectively, all the AX Series device's VLANs together cannot exceed the specified limit. **per-vlan-limit** – Limit applies to each VLAN. No individual can exceed the specified limit.
bcast | ipmcast | mcast | unknown_ucast	Specifies the type of traffic to limit: **bcast** – Broadcast traffic **ipmcast** – IP multicast traffic **mcast** – All multicast packets *except* IP multicast packets **unknown_ucast** – Unknown unicast traffic
num	Specifies the maximum number of packets per second that are allowed of the specified traffic type.

Default

The default per-VLAN limit for each type of traffic is 1000 packets per second. The default all-VLAN limit for each type of traffic is 5000 packets per second.

Mode

Configuration mode

Example The following command limits each VLAN to 1000 multicast packets per second:

```
AX(config)#system per-vlan-limit mcast 1000
```

system module-ctrl-cpu

Description Specify the maximum amount of control CPU that can be used at any given time for processing of CLI or SNMP output.

Syntax

```
[no] system module-ctrl-cpu
    {low | medium | high}
```

Default Not set

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 resource-usage

Description Change the capacity of a system resource.

Syntax

```
[no] system resource-usage resource-type maximum
```

Parameter	Description
resource-type	Specifies the system resource you are resizing: **class-list-ipv6-addr-count** – Maximum number of IPv6 addresses allowed within each IPv6 class list **client-ssl-template-count** – Total configurable client SSL templates **conn-reuse-template-count** – Total configurable connection reuse templates **fast-tcp-template-count** – Total configurable Fast TCP templates **fast-udp-template-count** – Total configurable Fast UDP templates

http-template-count – Total configurable HTTP templates

l4-session-count – Total Layer 4 sessions

nat-pool-addr-count – Total IP source NAT pools

persist-cookie-template-count – Total configurable persistent cookie templates

persist-srcip-template-count – Total configurable source IP persistence templates

proxy-template-count – Total configurable proxy templates

real-port-count – Total real server ports

real-server-count – Total real servers

server-ssl-template-count – Total configurable server SSL templates

service-group-count – Total service groups

stream-template-count – Total configurable streaming-media templates

virtual-port-count – Total virtual server ports

virtual-server-count – Total virtual servers

maximum The maximum number of the specified resource you want to allow on the AX Series.

Default The default maximum number for each type of system resource depends on the AX Series model. To display the defaults and current values for your AX Series, enter the following command: “show system resource-usage” on page 782.

Mode Configuration mode

Usage

The maximum number you can configure depends on the resource type and the AX Series model. To display the range of values that are valid for a resource, enter a question mark instead of a quantity.

- The maximum number of real servers allowed in a service group is half the total number of real servers allowed on the device.
- The maximum number of real ports allowed on a real server is half the total number of real ports allowed on the device.
- For all the following types of SLB templates, the total number allowed is 256 each, and is not configurable in the current release:
  - RAM caching
  - SIP
  - SMTP
  - Policy (PBSLB)
- The total number of health monitors allowed is 1024 and is not configurable.
- For every type of system resource that has a default, the AX device reserves one instance of the resource.

  For example, the device allows a total of 256 RAM caching templates. However, the device reserves one RAM caching template for the default template, which leaves a maximum of 255 additional RAM caching templates that can be configured.

Reload or Reboot Required

To place a change to l4-session-count into effect, a reboot is required. A reload will not place this change into effect. For changes to any of the other system resources, a reload is required but a reboot is not required.

Example

The following commands display the current usage and settings for maximum URI count, then display the range of values to which the default maximum can be set, then reset the default maximum to 512.

```
AX(config)#show system resource-usage
Resource                         Current    Default    Minimum    Maximum
--------------------------------------------------------------------------
l4-session-count                 8388608    8388608    524288     33554432
...
stream-uri-count                 256        256        32         1024
...
AX(config)system resource-usage stream-uri-count ?
  <32-1024>  Total configurable URI strings in the System
AX(config)system resource-usage stream-uri-count 512
Changes will take effect next time the software is reloaded.
```

system template

Description Globally applies a policy template to the AX device.

Syntax

```
[no] system template policy template-name
```

Default N/A

Mode Configuration mode

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`	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. – 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 AX 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 AX device differs depending on the AX model.
`system-mac`	Assigns the system MAC address (the MAC address of Ethernet data port 1) to all VEs. This method provides the same MAC assignment used in AX releases earlier than 2.6.1.

`hash-based`	Uses 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 AX model, regardless of the order in which VEs are configured.

Default **hash-based**

Mode Configuration mode

Usage A reload or reboot is required to place the change into effect.

system-reset

Description Restore the AX device to its factory default configuration.

Syntax

```
system-reset
```

Default N/A

Mode Configuration mode

Usage This command is helpful when you need to redeploy an AX 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 erases any saved configuration profiles, as well as system files such as SSL certificates and keys, and system logs. The management IP address and admin-configured admin and enable passwords are also removed.

However, the command does not remove the running-config and 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 AX device to erase the running-config and place the system reset into effect.

Example The following commands reset an AX device to its factory default configuration, then reboot the device to erase the running-config:

```
AX(config)#system-reset
AX(config)#end
AX#reboot
```

tacacs-server

Description

Configure TACACS+ for authorization and accounting. If authorization or accounting is specified, the AX 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 protocol-portnum]
[timeout seconds]
```

Parameter	Description
hostname | ipaddr	Hostname or IP address of the TACACS+ server. If a hostname is to be used, make sure a DNS server has been configured.
secret-string	Password, 1-128 characters, required by the TACACS+ server for authentication requests.
protocol-portnum	The port used for setting up a connection with a TACACS+ server.
seconds	The maximum number of seconds allowed for setting up a connection with a TACACS+ server. You can specify 1-12 seconds.

Default

The default port number is 49. The default timeout is 12 seconds.

Mode

Configuration mode

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":

```
AX(config)#tacacs-server host 192.168.3.45 secret SharedSecret
```

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:

```
AX(config)#tacacs-server host 192.168.3.72 secret NewSecret port 1980 timeout 6
```

The following command deletes TACACS+ server “192.168.3.45:

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

The following command deletes all TACACS+ servers:

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

techreport

Description

Configure automated collection of system information. If you need to contact Technical Support, they may ask you to for the techreports to help diagnose system issues.

Syntax

`[no] techreport {interval minutes | disable}`

Parameter	Description
interval *minutes*	Specifies how often to collect new information. You can specify 15-120 minutes.
disable	Disables automated collection of system information.

Default

Automated collection of system information is enabled by default. The default interval is 15 minutes.

Mode

Configuration mode

Usage

The AX device saves all techreport information for a given day in a single file. Timestamps identify when each set of information is gathered. The AX device saves techreport files for the most recent 31 days. Each day’s reports are saved in a separate file.

The techreports are a light version of the output generated by the **show techsupport** command. To export the information, use the **show techsupport** command. (See “show techsupport” on page 783.)

terminal

Description

Set the terminal configuration.

Syntax

```
[no] terminal {auto-size | editing | history
[size number] | idle-timeout minutes |
length number | no-ha-prompt | width lines}
```

Parameter	Description
auto-size	Automatically adjusts the length and width of the terminal display.
editing	Enables command editing.
history [**size** *number*]	Enables the command history and specifies the number of commands it can contain, 0-1000.
idle-timeout *minutes*	Specifies the number of minutes a CLI session can be idle before it times out and is terminated, 0-60 minutes. To disable timeout, enter 0.
length *number*	Specifies the number of lines to display per page, 0-512. To disable paging, enter 0.
no-ha-prompt	Disables display of the HA status in the CLI prompt. (For more information, see "High Availability Status in Command Prompt" on page 34.)
width *lines*	Specifies the number of columns to display, 0-512. To use an unlimited number of columns, enter 0.

Default

This command has the following defaults:

- **auto-size** – enabled
- **editing** – enabled
- **history** – enabled, for up to 256 commands
- **idle-timeout** – 10 minutes
- **length** – 24 lines
- **no-ha-prompt** – Disabled. (Display of the HA status is ***enabled***.)
- **width** – 80 columns

Mode

Configuration mode

Example

The following example sets the idle-timeout to 30 minutes:

```
AX(config)#terminal idle-timeout 30
```

tftp blksize

Description

Change the TFTP block size.

Syntax

```
[no] tftp blksize bytes
```

Parameter	Description
bytes	Maximum packet length the AX TFTP client can use when sending or receiving files to or from a TFTP server. You can specify from 512-32768 bytes.

Default

512 bytes

Mode

Configuration mode

Usage

Increasing the TFTP block size can provide the following benefits:

- TFTP file transfers can occur more quickly, since fewer blocks are required to a send a file.
- File transfer errors due to the server reaching its maximum block size before a file is transferred can be eliminated.

To determine the maximum file size a block size will allow, use the following formula:

1K-blocksize = 64MB-filesize

Here are some examples.

Block Size	Maximum File Size
1024	64 MB
8192	512 MB
32768	2048 MB

Increasing the TFTP block size of the AX device only increases the maximum block size supported by the AX 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.

Example

The following commands display the current TFTP block size, increase it, then verify the change:

```
AX(config)#show tftp
TFTP client block size is set to 512
AX(config)#tftp blksize 4096
AX(config)#show tftp
TFTP client block size is set to 4096
```

trunk

Description

Configure a trunk group, which is a single logical link consisting of multiple Ethernet ports.

Syntax

`[no] trunk Trunknum`

Parameter	Description
Trunknum	Specifies the trunk ID.

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

Command	Description
disable ethernet *portnum* [**to** *portnum*] [**ethernet** *portnum*] ...	Disables ports in the trunk.
enable ethernet *portnum* [**to** *portnum*] [**ethernet** *portnum*] ...	Enables ports in the trunk.
[**no**] **ethernet** *portnum* [**to** *portnum*] [**ethernet** *portnum*] ...	Adds ports to the trunk.

[no] ports-threshold *num*	Specifies the minimum number of ports that must be up in order for the trunk to remain up. You can specify 2-8. If the number of up ports falls below the configured threshold, the AX automatically disables the trunk's member ports. The ports are disabled in the running-config. The AX device also generates a log message and an SNMP trap, if these services are enabled.
[no] ports-threshold-timer *seconds*	Specifies how many seconds to wait after a port goes down before marking the trunk down, if the threshold is exceeded. You can set the ports-threshold timer to 1-300 seconds. The default is 10 seconds.

Default

N/A

Mode

Configuration mode

Usage

A maximum of 8 trunk groups are supported. Each group can have a maximum of 8 ports. Trunk group port numbers do not need to be consecutive.

Configuration of port-level parameters can be performed at the configuration level for the trunk.

Ports-Threshold

By default, a trunk's status remains UP so long as at least one of its member ports is up. You can change the ports threshold of a trunk to 2-8 ports.

If the number of up ports falls below the configured threshold, the AX automatically disables the trunk's member ports. The ports are disabled in the running-config. The AX device also generates a log message and an SNMP trap, if these services are enabled.

Note: After the feature has disabled the members of the trunk group, the ports are not automatically re-enabled. The ports must be re-enabled manually after the issue that caused the ports to go down has been resolved.

In some situations, a timer is used to delay the ports-threshold action. The configured port threshold is not enforced until the timer expires. The ports-threshold timer for a trunk is used in the following situations:

- When a member of the trunk links up.
- A port is added to or removed from the trunk.
- The port threshold for the trunk is configured during runtime. (If the threshold is set in the startup-config, the timer is not used.)

Example The following commands configure trunk 1 and add ports 6-8 and 14 to it:

```
AX(config)#trunk 1
AX(config-trunk:1)#ethernet 6 to 8 ethernet 14
```

Example The following commands configure an 8-port trunk, set the port threshold to 6, and display the trunk's configuration:

```
AX(config)#trunk 1
AX(config-trunk:1)#ethernet 1 to 8
AX(config-trunk:1)#ports-threshold 6
AX(config-trunk:1)#show trunk
Trunk ID         : 1       Member Count: 8
Trunk Status     : Up
Members          : 1   2   3   4   5   6   7   8
Cfg Status       : Enb Enb Enb Enb Enb Enb Enb Enb
Oper Status      : Up  Up  Up  Up  Up  Up  Up  Up
Ports-Threshold  : 6       Timer: 10 sec(s) Running: No
Working Lead     : 1
```

tx-congestion-ctrl

Description Configure looping on the polling driver, on applicable AX models.

Note: This command can impact system performance. It is recommended not to use this command unless advised by A10 Networks technical support.

Syntax `tx-congestion-ctrl` *retries*

Default 1

Mode Configuration mode

update

Description

Copy the currently running system image from the hard disk to the compact flash (cf).

Syntax Description

```
update cf {pri | sec}
```

Parameter	Description
pri | sec	Image to replace: **pri** – primary image **sec** – secondary image

Default

N/A

Mode

Configuration mode

Usage

This command does not save the configuration or reboot. To verify the update, enter the **show version** command.

Example

The following command copies the currently running system image from the hard disk to the secondary image area on the compact flash.

```
AX(config)#update cf sec
```

upgrade

Upgrade the system.

Syntax Description

```
upgrade {cf | hd} {pri | sec} [use-mgmt-port] url
```

Parameter	Description
cf | hd	System location to which write the upgrade image: **cf** – compact flash **hd** – hard drive
pri | sec	Image to replace: **pri** – primary image **sec** – secondary image
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 AX device attempts to use the data route table to reach the remote device through a data interface.

url — File transfer protocol, username (if required), and directory path.

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. The password can be up to 255 characters long.

To enter the entire URL:

tftp://*host***/***file*

ftp://[*user*@]*host*[:*port*]**/***file*

scp://[*user*@]*host***/***file*

rcp://[*user*@]*host***/***file*

Default N/A

Mode Configuration mode

Usage For complete upgrade instructions, see the release notes for the AX release to which you plan to upgrade.

There is no “**no**” form of this command.

Example The following example uses TFTP to upgrade the system image in the secondary image area of the hard disk:

```
AX(config)#upgrade hd sec tftp://192.168.1.144/ax2k_upg_1_2_0_107.tgz

Do you want to reboot the system after the upgrade?[yes/no]:yes
```

vlan

Description Configure a virtual LAN (VLAN). This command changes the CLI to the configuration level for the VLAN.

Syntax `[no] vlan vlan-id`

Parameter	Description
vlan-id	VLAN ID, from 1 to 4094.

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.

For information about the commands available at the VLAN configuration level, see “Config Commands: VLAN” on page 235.

Example

The following command adds VLAN 69 and enters the configuration level for it:

```
AX(config)#vlan 69
AX(config-vlan:69)#
```

web-service

Description

Configure access parameters for the Graphical User Interface (GUI).

Syntax

```
[no] web-service
{
auto-redir |
axapi-timeout-policy idle minutes |
port protocol-port |
secure-port protocol-port |
server |
secure-server |
timeout-policy idle minutes
}
```

Parameter	Description
auto-redir	Enables requests for the unsecured port (HTTP) to be automatically redirected to the secure port (HTTPS).
axapi-timeout-policy idle *minutes*	Specifies the number of minutes an aXAPI session can remain idle before being terminated. Once the aXAPI session is terminated, the session ID generated by the AX device for the session is no longer valid. You can specify 0-60 minutes. If you specify 0, sessions never time out.

Note: The **axapi-timeout-policy** option is not applicable to IPv6 migration.

port *protocol-port*	Specifies the protocol port number for the unsecured (HTTP) port.
secure-port *protocol-port*	Specifies the protocol port number for the secure (HTTPS) port.
server	Enables the HTTP server.
secure-server	Enables the HTTPS server.
timeout-policy idle *minutes*	Specifies the number of minutes a Web management session can remain idle before it times out and is terminated by the AX device. You can specify 0-60 minutes. To disable the timeout, enter 0.

Default

This command has the following defaults:

- **auto-redir** – enabled
- **axapi-timeout-policy idle** – 5 minutes
- **port** – 80
- **secure-port** – 443
- **server** – enabled
- **secure-server** – enabled
- **timeout-policy** – 10 minutes

Mode

Configuration mode

Usage

If you disable HTTP or HTTPS access, any sessions on the management GUI are immediately terminated.

Example

The following command disables management access on HTTP:

```
AX(config)#no web-service server
```

write

Description

Write the running-config to a configuration profile. (See "write" on page 77.)

write terminal

Description Display the running-config on the terminal. (See "write terminal" on page 78.)

Config Commands: Interface

This chapter describes the commands for configuring AX interface parameters.

To access this configuration level, enter the following command at the Global Config level:

```
interface {ethernet port-num | ve ve-num |
loopback num | management | trunk num}
```

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

access-list

Description

Apply an Access Control List (ACL) to an interface.

Syntax

```
[no] access-list acl-num in
```

Parameter	Description
acl-num	Number of a configured ACL.
in	Applies the ACL to inbound traffic received on the interface.

Default

N/A

Mode

Interface

Usage

The ACL must be configured before you can apply it to an interface. To configure an ACL, see "access-list (standard)" on page 80 and "access-list (extended)" on page 82.

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 AX Series 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:

```
AX(config)#access-list 1 deny 10.10.10.0 0.0.0.255
AX(config)#interface ethernet 4
AX(config-if:ethernet4)#access-list 1 in
```

bfd

Description

Enable or disable BFD on an individual interface.

Syntax

`[no] bfd {authentication | echo | interval}`

Parameter	Description
authentication *key-id* {**md5** | **meticulous-md5** | **meticulous-sha1** | **sha1** | **simple**}	The **authentication** option specifies the authentication type to be used for BFD. You can specify a *key-id* from 0-255. The authentication options include the following: **md5** – Keyed MD5 **meticulous-md5** – Meticulous keyed MD5 **meticulous-sha1** –Meticulous keyedSHA1 **sha1** – Keyed SHA1 **simple** – Simple password
echo [**demand**]	Specify **echo** mode. You can enable the **demand** mode to work in conjunction with the echo func-

tion. When demand mode is enabled (and a BFD session has been established), the system will be able to verify connectivity with another system at will instead of routinely.

interval *ms*
min-rx *ms*
multiplier *num*

The **interval** value is the transmit timer, and it specifies the rate at which the AX 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 number of *ms* the AX 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 AX device will wait for a BFD control packet from a neighbor. If the multiplier value is reached, the AX device concludes that the routing process on the neighbor is down. The **multiplier** value can be 3-50 and is 4 by default.

Mode

Interface

bcast-rate-limit (management interface only)

Description

Limit the amount of broadcast traffic the AX device accepts on the management port. If the rate of broadcast traffic to the AX device' management port exceeds the default or configured rate, the AX device drops the over-limit traffic.

Syntax

```
[no] bcast-rate-limit rate pkts-per-sec
```

Parameter	Description
rate	Limits the amount of broadcast traffic accepted on the management interface.
pkts-per-sec	Specifies the rate, which can be 50-5000. If you do not specify a rate, the rate is set to 500 broadcast packets per second.

Default 500

Introduced in Release 2.6.6-P6

Mode Interface

Usage A built-in rate limit for the management port is always enforced to prevent the port from becoming unresponsive due to excessive traffic. This command allows you to change the broadcast-rate limit for the management port to configure additional, more restrictive rate limiting.

Example The following commands access the management port and configure a broadcast-rate limit of 654 broadcast packets per second:

```
AX-Active(config)#interface management
AX-Active(config-if:management)#bcast-rate-limit rate 655
The broadcast rate limit is rounded down to 654
```

cpu-process

Description Enable software-based switching or routing of Layer 2/Layer 3 traffic.

Note: This command is applicable only to models that have the flexible traffic ASIC.

Syntax `[no] cpu-process`

Default Disabled. Traffic is switched or routed in hardware.

Mode Interface

disable

Description

Disable an interface.

Syntax

```
disable
```

Default

The management interface is enabled by default. Data interfaces are disabled by default.

Mode

Interface

Usage

This command applies to all interface types: Ethernet data interfaces, out-of-band Ethernet management interface, Virtual Ethernet (VE) interfaces, and loopback interfaces.

The command also applies to trunks. When you disable a trunk at the interface configuration level for the trunk, Layer 3 forwarding is disabled on the trunk.

Example

The following command disables Ethernet interface 3:

```
AX(config-if:ethernet3)#disable
```

Example

The following commands access the interface configuration level for trunk 7 and disable Layer 3 forwarding on the trunk:

```
AX(config)#interface trunk 7
AX(config-if:trunk7)#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:

```
AX(config-if:ethernet6)#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.

Example

The following command enables Ethernet interface 3:

```
AX(config-if:ethernet3)#enable
```

flow-control

Description

Enable 802.3x flow control on a full-duplex Ethernet interface.

Syntax

```
[no] flow-control
```

Default

Disabled. The AX Ethernet interface auto-negotiates flow control settings with the other end of the link.

Mode

Interface

Usage

This command can cause the interface to briefly go down, then come back up again.

icmp-rate-limit

Description

Configure ICMP rate limiting, to protect against denial-of-service (DoS) attacks.

Syntax

```
[no] icmp-rate-limit normal-rate lockup max-rate
lockup-time
```

Parameter	Description
normal-rate	Maximum number of ICMP packets allowed per second on the interface. If the AX 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.
lockup *max-rate*	Maximum number of ICMP packets allowed per second before the AX device locks up ICMP traffic on the interface. When ICMP traffic is locked up, all ICMP packets on the interface are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.
lockup-time	Number of seconds for which the AX 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 ICMP rate limiting globally, see "icmp-rate-limit" on page 131. To configure it in a virtual server template, see "slb template virtual-server" on page 640. 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 configures ICMP rate limiting on Ethernet interface 3:

```
AX(config-if:ethernet3)#icmp-rate-limit 1024 lockup 1200 10
```

interface

Description Access the interface configuration level for another interface.

Syntax

```
interface {ethernet port-num | ve number |
loopback number | trunk num | management}
```

Default N/A

Mode Interface

Usage This command allows you to go directly to the configuration level for another interface, without the need to return to the global Config level first.

Example The following command changes the CLI from the configuration level for Ethernet interface 3 to the configuration level for Ethernet interface 4:

```
AX(config-if:ethernet3)#interface ethernet 4
AX(config-if:ethernet4)#
```

ip address

Description Assign 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 AX Series 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 AX devices deployed in gateway (route) mode.

Each IP address must be unique on the AX device. Addresses within a given subnet can be configured on only one interface on the device. (The AX 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 AX 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.

Example The following command assigns IP address 10.2.4.69 to Ethernet interface 9:

```
AX(config-if:ethernet9)#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.

```
AX(config)#interface ethernet 1
AX(config-if:ethernet1)#ip address 10.10.10.1 /24
AX(config-if:ethernet1)#ip address 10.10.20.2 /24
AX(config-if:ethernet1)#ip address 20.20.20.1 /24
AX(config-if:ethernet1)#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
AX(config-if:ethernet1)#no ip address 10.10.20.2 /24
AX(config-if:ethernet1)#show ip interfaces ethernet 1
  Ethernet 1 ip addresses:
  10.10.10.1 /24 (Primary)
  20.20.20.1 /24
```

ip control-apps-use-mgmt-port (management interface only)

Description

Enable use of the management interface as the source interface for automated management traffic.

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 AX 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 AX device attempts to use a route from the main route table for management connections originated on the AX device. The **ip control-apps-use-mgmt-port** command enables the AX device to use the management route table for these connections instead.

The AX device will use the management route table for reply traffic on connections initiated by a remote host that reaches the AX device on the management port. For example, this occurs for SSH or HTTP connections from remote hosts to the AX device.

Example

The following command enables use of the management interface as the source interface for automated management traffic:

```
AX(config-if:management)#ip control-apps-use-mgmt-port
```

ip default-gateway (management interface only)

Description

Specify the default gateway for the out-of-band management interface.

Syntax

```
[no] ip default-gateway ipaddr
```

Default

None

Mode

Interface

Configuring a default gateway for the management interface provides the following benefits:

- Ensures that reply management traffic sent by the AX Series 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 AX is deployed in transparent mode) or an IP route is used (if the AX is deployed in route mode).

To configure the default gateway for data interfaces on an AX Series device deployed in transparent mode, use the **ip default-gateway** command at the global Config level. (See "ip address" on page 211.)

Note: Normally, if the AX 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:

- For automated management traffic such as syslog messages and SNMP traps, see "ip control-apps-use-mgmt-port (management interface only)" on page 212.

- 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:

```
AX(config)#interface management
AX(config-if:management)#ip address 10.10.20.1 /24
AX(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`

Parameter	Description
ipaddr	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 AX interface on which the helper address is configured must have an IP address.

The helper address can not be the same as the IP address on any AX 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 AX 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.

```
AX(config)#interface ethernet 1
AX(config-if:ethernet1)#ip helper-address 100.100.100.1
AX(config-if:ethernet1)#interface ve 5
AX(config-if:ve5)#ip helper-address 100.100.100.1
AX(config-if:ve5)#interface ve 7
AX(config-if:ve7)#ip helper-address 100.100.100.1
AX(config-if:ve7)#interface ve 9
AX(config-if:ve9)#ip helper-address 20.20.20.102
```

ip nat

Description Enable source Network Address Translation (NAT) on an interface.

Syntax

```
[no] ip nat {inside | outside}
```

Parameter	Description
`inside`	Specifies that this AX 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 AX interface is connected to the external network or Internet. Before sending traffic from an inside host out on this interface, the AX device translates the host's private address into a public, routable address.

Default None

Mode Interface

Usage On an AX device deployed in transparent mode, this command is valid only on Ethernet data ports. On an AX 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. See the **ip nat** commands in "Config Commands: IP" on page 239.

In addition, on some AX models, if Layer 2 IP NAT is required, you also must enable CPU processing on the interface. (See "cpu-process" on page 206.) This applies to models AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200.

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.

```
AX(config)#access-list 3 permit 10.1.1.0 0.0.0.255
AX(config)#ip nat pool 1 10.153.60.120 10.153.60.150 netmask /24
AX(config)#ip nat inside source list 3 pool 1
AX(config)#interface ethernet 14
AX(config-if:ethernet14)#ip address 10.1.1.1 255.255.255.0
AX(config-if:ethernet14)#ip nat inside
AX(config-if:ethernet14)#interface ethernet 15
AX(config-if:ethernet15)#ip address 10.153.60.100 255.255.255.0
AX(config-if:ethernet15)#ip nat outside
```

ip ospf

Description

Configure IPv4 Open Shortest Path First (OSPF) parameters on a data interface. See "ip ospf" on page 338.

ip rip

Description

Configure interface-level parameters for IPv4 Routing Information Protocol (RIP). See "Interface-Level IPv4 RIP Commands" on page 293.

{ip | ipv6} router isis

Description

Enable Intermediate System to Intermediate System (IS-IS) routing on a data interface.

Syntax

`[no] {ip | ipv6} router isis [tag]`

Default

Not set

Mode

Interface

{ip | ipv6} stateful-firewall

Description

Enable stateful-firewall support on a data interface.

Syntax

```
[no] {ip | ipv6} stateful-firewall
{inside | outside [access-list num]}
```

Parameter	Description
`ip	ipv6`	IP version.
`inside	outside`	Traffic direction.
`access-list id`	ACL ID.

Default

Not set

Introduced in Release

2.6.6-P4

Mode

Interface

ipv6 (on management interface)

Description

Configure an IP version 6 address and default gateway on the management interface.

Syntax

```
[no] ipv6 address ipaddr/mask-length
```

Syntax

```
[no] ipv6 default-gateway gateway-ipaddr
```

Default

None.

Mode

Interface

Usage

The **ipv6 default-gateway** command applies only to the management interface. To configure IPv6 on a data interface, see “ipv6 address” on page 218.

Example

The following commands configure an IPv6 address and default gateway on the management port:

```
AX(config-if:management)#ipv6 address 2001:db8:11:2/32
AX(config-if:management)#ipv6 default-gateway 2001:db8:11:1/32
```

ipv6 access-list

Description Apply an IPv6 Access Control List (ACL) to an interface.

Syntax

```
[no] ipv6 access-list name in
```

Parameter	Description
name	Name of a configured IPv6 ACL.
in	Applies the ACL to inbound IPv6 traffic received on the interface.

Default N/A

Mode Interface

ipv6 address

Description Configure an IPv6 address on the interface.

Syntax

```
[no] ipv6 address ipaddr/prefix-length
[link-local] [any-cast]
```

Parameter	Description
ipv6-addr	Valid unicast IPv6 address.
prefix-length	Prefix length, up to 128.
link-local	Configures the address as the link-local IPv6 address for the interface, instead of a global address. Without this option, the address is a global address.
any-cast	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.

To configure IPv6 on the management interface, see "ipv6 (on management interface)" on page 217.

Example The following command configures a global IPv6 address on Ethernet interface 8:

```
AX(config-if:ethernet8)#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:

```
AX(config-if:ethernet6)#ipv6 address fe80::1/64 link-local
```

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.

To manually configure the address instead, see "ipv6 address" on page 218.

Example The following command enables an automatically generated link-local IPv6 address on Ethernet interface 6:

```
AX(config-if:ethernet6)#ipv6 enable
```

ipv6 nat inside

Description Enable inside NAT on the interface.

Syntax `[no] ipv6 nat inside`

Default Disabled

Mode Configuration mode

ipv6 nat outside

Description Enable outside NAT on the interface.

Syntax

```
[no] ipv6 nat outside
```

Default Disabled

Mode Configuration mode

ipv6 ndisc router-advertisement

Description Configure IPv6 router discovery (RFC 4861).

Syntax

```
[no] ipv6 ndisc router-advertisement
{
default-lifetime seconds |
disable |
enable |
ha-group-id group-id
  [use-floating-ip ipv6-addr/prefix-length] |
hop-limit num |
managed-configuration-flag {disable | enable} |
max-interval seconds |
min-interval seconds |
mtu {disable | bytes} |
other-configuration-flag {disable | enable} |
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
}
```

Parameter	Description
default-lifetime *seconds*	Specifies the number of seconds for which router advertisements sent on this interface are valid. You can specify 0 or 4-9000 seconds. The value

can not be less than the maximum advertisement interval. If you specify 0, the host will not use this interface (IPv6 router) as a default route.

disable Disables IPv6 router discovery.

enable Enables IPv6 router discovery.

ha-group-id *group-id* [**use-floating-ip** *ipv6-addr/prefix-length*] Specifies an HA group for which to send router advertisements.

The **use-floating-ip** option specifies a floating IPv6 address to use as the source address for router advertisements for the HA group. The address must be a link-local address on this interface. The HA virtual MAC address will be used as the source address.

hop-limit *num* Specifies the default hop count value that should be used by hosts. For a given packet, the 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.

managed-configuration-flag {**disable** | **enable**} Enables or disables the M (managed) flag in IPv6 router advertisements. The M flag instructs clients to use DHCPv6 or some other stateful method to acquire an IPv6 address.

max-interval *seconds* Specifies the maximum number of seconds between transmission of unsolicited router advertisement messages on this interface. You can specify 4-1800 seconds.

min-interval *seconds* Specifies the minimum number of seconds between transmission of unsolicited router advertisement messages on this interface. You can specify 3-1350 seconds.

mtu {disable | *bytes*}

Specifies the MTU value to include in the MTU options field. You can specify 1200-1500 bytes (on 1-Gbps interfaces) or **disabled**.

Note: If the option is disabled, no MTU value is included.

other-configuration-flag {disable | enable}

Enables or disables the O (other) flag in IPv6 router advertisements. The O flag instructs clients to use DHCPv6 or some other stateful method to acquire other information, such as DNS server IPv6 addresses.

Note: Here, “other” information means information other than the clients’ IPv6 address. To instruct clients to use DHCPv6 or some other stateful method to acquire an IPv6 address, enable the M (managed) flag. (See the description above for the **managed-configuration-flag** option.)

prefix *ipv6-addr/prefix-length* [*options*]

Specifies the IPv6 prefixes to advertise on this interface. A maximum of 32 prefixes can be advertised on an interface.

The following options are supported:

not-autonomous – Disables support for auto-configuration of IPv6 addresses by clients.

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).

preferred-lifetime *seconds* – Specifies the number of seconds for which auto-generated addresses remain preferred. You can specify 0-4294967295 seconds. The default is 604800.

valid-lifetime *seconds* – specifies the number of seconds for which advertisement of the prefix is valid. You can specify 1-4294967295 seconds. The default is 2592000.

rate-limit *num*	Specifies the maximum number of router solicitation requests per second that will be processed on the interface. You can specify 1-100000 messages per second.
reachable-time *ms*	Specifies the number of milliseconds (ms) for 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.
retransmit-timer *seconds*	Specifies the number of seconds a host should wait between sending neighbor solicitation messages. You can specify 0-4294967295 seconds. If you specify 0, the value is unspecified by this IPv6 router.

Default

IPv6 router discovery is disabled by default. The command options have the following default values:

- **default-lifetime** – 1800 seconds
- **disable** – Disabled
- **enable** – Disabled
- **ha-group-id** – Not set. Advertisements are sent regardless of HA group.
- **hop-limit** – 255
- **managed-configuration-flag** – Disabled
- **max-interval** – 600 seconds
- **min-interval** – 200 seconds
- **mtu** – disabled
- **other-configuration-flag** – Disabled
- **prefix** – All prefixes for IPv6 addresses that are configured on this interface are advertised. The prefix options have the following defaults:
  - **not-autonomous** – disabled (Auto-configuration of IPv6 addresses by clients is enabled.)
  - **not-on-link** – enabled (On-Link is disabled.)
  - **preferred-lifetime** – 604800 seconds
  - **valid-lifetime** – 2592000 seconds
- **rate-limit** – 100000 messages per second

- **reachable-time** – 0 (The value is unspecified by this IPv6 router.)
- **retransmit-timer** – 0 (The value is unspecified by this IPv6 router.)

Mode

Interface

Usage

When router discovery is enabled, the AX 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 AX 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 AX 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 AX 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 AX 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.

```
AX(config)#interface ethernet 1
AX(config-if:ethernet1)#ipv6 address 2001::1/64
AX(config-if:ethernet1)#ipv6 ndisc router-advertisement enable
AX(config-if:ethernet1)#ipv6 ndisc router-advertisement max-interval 300
AX(config-if:ethernet1)#ipv6 ndisc router-advertisement min-interval 150
AX(config-if:ethernet1)#ipv6 ndisc router-advertisement prefix 2001::/64
on-link
AX(config-if:ethernet1)#ipv6 ndisc router-advertisement prefix 2001:a::/96
on-link
```

ipv6 ospf

Description Configure Open Shortest Path First (OSPF) parameters on an IPv6 data interface. See “Interface-level Configuration Commands” on page 338.

ipv6 rip split-horizon

Description Configure the split-horizon method IPv6 Routing Information Protocol (RIP). See “ipv6 rip split-horizon” on page 307.

ipv6 router isis

Description Configure options for Intermediate System to Intermediate System (IS-IS) on an IPv6 data interface.

Syntax

```
[no] ipv6 router isis [options]
```

Default None

Mode Interface

ipv6 router ospf

Description Configure an OSPFv3 area on an IPv6 data interface.

Syntax

```
[no] ipv6 router ospf
{
area {num | ipaddr} [tag tag [instance-id num]] |
tag tag area {num | ipaddr} [instance-id num]
}
```

Default None

Mode Interface

ipv6 router rip

Description Enable Routing Information Protocol (RIP) on an IPv6 data interface.

Syntax

```
[no] ipv6 router rip
```

Default None

Mode Interface

isis

Description Configure interface-level parameters for Intermediate System to Intermediate System (IS-IS). See “Interface-level IS-IS Configuration Commands” on page 380.

l3-vlan-fwd-disable

Description Disable Layer 3 forwarding between VLANs on tis interface.

Syntax

```
[no] l3-vlan-fwd-disable
```

Default By default, the AX device can forward Layer 3 traffic between VLANs.

Mode Interface

Usage This command is applicable only on AX devices deployed in gateway (route) mode. If the option to disable Layer 3 forwarding between VLANs is configured at any level, the AX device can not be changed from gateway mode to transparent mode, until the option is removed.

The command is applicable to ***inbound*** traffic on the interface.

The command is valid on physical Ethernet interfaces, Virtual Ethernet (VE) interfaces, trunks, and on the lead interface in trunks.

However, if the command is configured on a physical Ethernet interface, that interface can not 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.

To display statistics for this option, see “show slb switch” on page 772.

lacp port-priority

Description Set the Link Aggregation Control Protocol (LACP) priority of the interface.

Syntax

```
[no] lacp port-priority num
```

Parameter	Description
num	Specifies the 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 Interface

Usage If the LACP trunk has more candidate members than are allowed by the device at the other end of the link, LACP selects the interfaces with the highest port priority values as the active interfaces. The other interfaces are standbys, and are used only if an active interface goes down.

lacp timeout

Description Set the aging timeout for LACP data units from the other end of the LACP link.

Syntax

```
[no] lacp timeout {short | long}
```

Parameter	Description
`short | long`	Specifies the timeout: **short** – 3 seconds **long** – 90 seconds

Default **long**

Mode Interface

lacp trunk

Description

Add the interface to an LACP trunk.

Syntax

```
[no] lacp trunk lacp-trunk-id [admin-key num]
mode {active | passive}
[unidirectional-detection]
```

Parameter	Description
lacp-trunk-id	Specifies the trunk ID, 1-16.
admin-key *num*	Specifies the key value for the trunk, 10000-65535. The admin key must match on all interfaces in the trunk.
mode {active | passive}	Specifies whether LACP will run in active or passive mode on the interface. **active** – Initiates link formation with the other end of the link. **passive** – Waits for the other end of the link to initiate link formation.
unidirectional-detection	Enables Unidirectional Link Detection (UDLD). UDLD checks the links in LACP trunks to ensure that both the send and receive sides of each link are operational.

Default

No LACP trunks are configured by default. When you add an interface to an LACP trunk, it has the following defaults:

- *lacp-trunk-id* – not set
- **admin-key** – 1000 plus the trunk ID. For example, for trunk 3, the default admin-key is “1003”.
- **mode** – **active**
- **unidirectional-detection** – disabled

Mode

Interface

Usage

The AX Series UDLD uses LACP protocol packets as heartbeat messages. If an LACP link on the AX device does not receive an LACP protocol packet within a specified timeout, LACP blocks traffic on the port. This corrects the problem by forcing the devices connected by the non-operational link to use other, fully operational links.

A link that is blocked by LACP can still receive LACP protocol packets but blocks all other traffic.

lacp udld-timeout

Description

Set the timeout interval for receiving LACP protocol packets from other ports.

Syntax

```
[no] lacp udld-timeout {fast | slow} num
```

Parameter	Description
`fast | slow`	Specifies the time unit: **fast** – Allows the timeout to be set in increments of milliseconds (ms). In this case, the *num* value can be 100-1000. **slow** – Allows the timeout to be set in increments of seconds. In this case, the *num* value can be 1-60.
num	Specifies the timeout. For supported values, see above.

Default

slow 1

Mode

Interface

Usage

The local port waits for the UDLD timeout to receive an LACP protocol packet from the remote port. If an LACP protocol packet does not arrive before the timeout expires, LACP disables the local port.

load-interval

Description

Change the interval for utilization statistics for the interface.

Syntax

```
[no] load-interval seconds
```

Parameter	Description
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.

To display interface utilization statistics, see and “show interfaces” on page 725 and “show statistics” on page 780.

Example

The following command changes the utilization statistics interval for Ethernet interface 1 to 200 seconds:

```
AX(config-if:ethernet1)#load-interval 200
```

lw-406

Description

Enable Lightweight 4over6 support on the interface.

Syntax

```
[no] lw-4o6 {inside | outside}
```

Parameter	Description
inside | outside	Traffic direction.

Default

Not set

Mode

Interface

monitor

Description

Configure an Ethernet interface to send a copy of its traffic to another Ethernet interface.

Syntax

```
[no] monitor [both | input | output]
```

Parameter	Description
both | input | output	Traffic direction to mirror. If you do not specify a direction, traffic in both directions is copied.

Default By default, no traffic is mirrored. When you enable a port to be monitored, both traffic directions are mirrored by default.

Mode Interface

Usage This command is valid only on Ethernet data interfaces. To specify the port to which to mirror the traffic, use the **mirror-port** command at the global Config level. (See “mirror-port” on page 149.)

Note: Only one mirror port is supported. All mirrored traffic for the directions you specify goes to that port.

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:

```
AX(config)#mirror-port ethernet 3
AX(config)#interface ethernet 5
AX(config-if:ethernet5)#monitor input
```

mtu

Description Change the Maximum Transmission Unit (MTU) for an Ethernet interface.

Syntax `[no] mtu bytes`

Parameter	Description
bytes	Largest packet size that can be forwarded out the interface. You can specify 1200-1500 bytes.

Default 1500 bytes

Mode Interface

Usage This command applies to the management interface and Ethernet data interfaces.

If the AX device needs to forward a packet that is larger than the MTU of the AX egress interface to the next hop, but the Do Not Fragment bit is set in the packet, the AX 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 AX device silently drops the packet.

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.

name

Description Assign a name to the interface.

Syntax

```
[no] name string
```

Parameter	Description
string	Name for the interface, 1-63 characters.

Default None

Mode Interface

Usage This command applies to physical and virtual Ethernet data interfaces, 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:

```
AX(config)#interface ve 1
AX(config-if:ve1)#name WLAN-interface
AX(config-if:ve1)#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
```

ospf

Description Configure OSPF on the interface. (See “Interface-level Configuration Commands” on page 338.)

speed

Description Set the maximum speed on an Ethernet interface.

Syntax

```
[no] speed {10 | 100 | 1000 | 10000 | auto}
```

Parameter	Description
10	10 Megabits per second (Mbs/sec)
100	100 Megabits per second (Mbs/sec)
1000	1 Gigabit per second (Gb/sec)
10000	10 Gigabits per second (Gbs/sec)
auto	The interface speed is negotiated based on the speed of the other end of the link.

Default **auto**

Mode Interface

Usage This command applies to the management interface and Ethernet data interfaces.

Example The following command changes the speed of Ethernet interface 6 to 10 Mbs/sec:

```
AX(config-if:ethernet6)#speed 10
```

Config Commands: VLAN

The commands in this chapter configure parameters on individual VLANs.

To access this CLI level, enter the **vlan** *vlan-id* command from the global Config level.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

name

Description Assign a name to the VLAN.

Syntax `[no] name string`

Parameter	Description
string	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:

```
AX(config)#vlan 100
AX(config-vlan:100)#name Test100
AX(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`

Parameter	Description
ve-num	VE number, 1-4094. 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 AX 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 AX device’s physical Ethernet data ports also are used for VEs. (See “system ve-mac-scheme” on page 189.)

Example

The following command configures VE 4 on VLAN 4:

```
AX(config-vlan:4)#router-interface ve 4
```

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
  [ethernet port-num ... | to port-num] |
tagged trunk num [trunk num ... | to num]
}
```

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:

```
AX(config-vlan:4)#tagged ethernet 4 to 5
```

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
  [ethernet port-num ... | to port-num] |
tagged trunk num [trunk num ... | to num]
}
```

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 to VLAN 4 as an untagged port:

```
AX(config-vlan:4)#untagged ethernet 6
```

Config Commands: IP

The IP commands configure global IPv4 parameters.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Note: To configure global IPv6 parameters, see “Config Commands: IPv6” on page 265.

ip anomaly-drop

Description Enable protection against distributed denial-of-service (DDoS) attacks.

Syntax `[no] ip anomaly-drop anomaly-type`

Parameter	Description
anomaly-type	Specifies the type of IP anomaly to protect against: **bad-content** [*threshold*] – Checks for invalid HTTP or SSL payloads in new HTTP or HTTPS connection requests from clients. (For more information, see “IP Anomaly Filters Used for System-Wide Policy-Based SLB” in the “Usage” section below.)

drop-all – Enables all the DDoS protection options listed below.

frag – Drops all IP fragments, which can be used to attack hosts running IP stacks that have known vulnerabilities in their fragment reassembly code.

ip-option – Drops all packets that contain any IP options.

land-attack – Drops spoofed SYN packets containing the same IP address as the source and destination, which can be used to launch an "IP land attack".

out-of-sequence [*threshold*] – Checks for out-of-sequence packets in new HTTP or HTTPS connection requests from clients. (For more information, see "IP Anomaly Filters Used for System-Wide Policy-Based SLB" in the "Usage" section below.)

ping-of-death – Drops all jumbo IP packets longer than the maximum valid IP packet size (65535 bytes), known as "ping of death" packets.

Note: On models AX 1000, AX 2000, AX 2100, AX 2500, AX 2600, and AX 3000, the **ping-of-death** option drops all IP packets longer than 32000 bytes. On models AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200, the option drops IP packets longer than 65535 bytes.

tcp-no-flag – Drops all TCP packets that do not have any TCP flags set.

tcp-syn-fin – Drops all TCP packets in which both the SYN and FIN flags are set.

tcp-syn-frag – Drops incomplete (fragmented) TCP Syn packets, which can be used to launch TCP Syn flood attacks.

zero-window [*threshold*] – Checks for a zero-length TCP window in new HTTP or HTTPS connection requests from clients. (For more information, see "IP Anomaly Filters Used for System-Wide Policy-Based SLB" in the "Usage" section below.)

Default All IP anomaly drop options are disabled by default.

Mode Configuration mode

Usage

All filters are supported for IPv4. All filters except **ip-option** are supported for IPv6.

On models AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200, DDoS protection is hardware-based. On other models, DDoS protection is software-based.

DDoS protection applies only to Layer 3, Layer 4, and Layer 7 traffic. Layer 2 traffic is not affected by the feature.

IP Anomaly Filters Used for System-Wide Policy-Based SLB

The bad-content, out-of-sequence, and zero-window filters apply only to system-wide Policy-Based SLB (PBSLB).

Filtering for these anomalies is disabled by default. However, if you configure a system-wide PBSLB policy, the filters are automatically enabled. You also can configure the filters on an individual basis.

Each of these filters has a configurable threshold. The threshold specifies the number of times the anomaly is allowed to occur in a client's connection requests. If a client exceeds the threshold, the AX device applies the system-wide PBSLB policy's over-limit action to the client.

For each of the new IP anomaly filters, the threshold can be set to 1-127 occurrences of the anomaly. The default is 10.

Note: The thresholds are not tracked by PBSLB policies bound to individual virtual ports.

The AX device tracks each of these types of anomaly for each client in each black/white list. For dynamic black/white-list clients, the statistics counters for these anomalies are reset to 0 when the client's dynamic entry ages out.

Example

The following command enables DDoS protection against ping-of-death attacks:

```
AX(config)#ip anomaly-drop ping-of-death
```

ip as-path

Description

Configure an AS-path list for BGP.

Syntax

```
[no] ip as-path access-list
regular-expression {deny | permit}
```

Parameter	Description
regular-expression	Access list name.
deny | **permit**	Action to perform on matching entries.

Default None

Mode Configuration mode

ip community-list

Description Specify BGP community attributes.

Syntax

```
[no] ip community-list num
{deny | permit}
[community-number]
[local-AS]
[no-advertise]
[no-export]
```

Syntax

```
[no] ip community-list {expanded | standard}
list-name
{deny | permit}
[community-number]
[local-AS]
[no-advertise]
[no-export]
```

Parameter	Description
num	List number.
{**expanded** | **standard**} *list-name*	List type and name.
deny | **permit**	Action to perform for matching communities.
community-number	Community number.
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

ip dns

Description Configure DNS servers and the default domain name (DNS suffix) for hostnames on the AX 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.

Example The following command sets primary DNS server 20.20.20.5:

```
AX(config)#ip dns primary 20.20.20.5
```

ip extcommunity-list

Description Configure an extended community list for BGP.

Syntax

```
[no] ip community-list num
{deny | permit}
{rt | soo {AS-num:nn | ipaddr:nn}}
```

Syntax

```
[no] ip community-list
{expanded | standard} list-name
{deny | permit}
{rt | soo {AS-num:nn | ipaddr:nn}}
```

Parameter	Description
num	List number.
{expanded | standard} *list-name*	List type and name.
deny | permit	Action to perform for matching communities.

`rt	soo {AS-num:nn	ipaddr:nn}`	Community type and ID: **rt** – Route-target extended community. **soo** – Site-of-origin extended community.

Default None

Mode Configuration mode

ip frag max-reassembly-sessions

Description Configure the IP fragment queue size.

Syntax

```
[no] ip frag max-reassembly-sessions num
```

Parameter	Description
num	specifies the maximum number of simultaneous fragmentation sessions the AX device will allow. You can specify 1-200000. The specified maximum applies to both IPv4 and IPv6.

Default 100000

Mode Configuration mode

ip frag timeout

Description Configure the timeout for IP packet fragments.

Syntax

```
[no] ip frag timeout ms
```

Parameter	Description
ms	Specifies the number of milliseconds (ms) the AX 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 4-16000 ms (16 seconds), in 10-ms increments.

Default 1000 ms (1 second)

Mode Configuration mode

ip icmp disable

Description Disable ICMP messages.

Syntax

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

Parameter	Description
`redirect`	Disables sending of ICMP Redirect messages.
`unreachable`	Disables sending of ICMP Destination Unreachable messages.

Default Both types of ICMP messages are enabled.

Mode Configuration mode

Usage The following command disables sending of IPv4 ICMP Redirect messages:

```
AX(config)#ip icmp disable redirect
```

ip nat alg pptp

Description Disable or re-enable 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 AX 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

ip nat allow-static-host

Description Enable static Network Address Translation (NAT).

Syntax

```
[no] ip nat allow-static-host
```

Default Disabled

Mode Configuration mode

Usage This command is required only if you configure individual static source mappings, using the **ip nat inside source static** command. If you configure a static range list instead, you do not need the **ip nat allow-static-host** command.

Example The following command enables static NAT support:

```
AX(config)#ip nat allow-static-host
```

ip nat icmp always-source-nat-errors

Description Enable NAT for ICMP messages from inside routers.

Syntax `[no] ip nat icmp always-source-nat-errors`

Default By default, the AX device does not translate the source IP addresses of ICMP error messages sent by inside routers into NAT addresses.

Introduced in Release 2.6.6-P6

Mode Configuration mode

ip nat icmp respond-to-ping

Description Enable ping replies from NAT pool addresses.

Syntax `[no] ip nat icmp respond-to-ping`

Default By default, the AX device does not reply to ping requests that are sent to NAT addresses (LSN NAT pool addresses). Instead, by default, the AX device drops ping requests sent to LSN NAT pool addresses.

Introduced in Release 2.6.6-P6

Mode Configuration mode

ip nat inside

Description

Configure inside Network Address Translation (NAT).

Syntax

```
[no] ip nat inside source
{
class-list name |
list acl-name pool pool-or-group-name |
static inside-ipaddr nat-ipaddr
[ha-group-id group-id]
[vrid {num | default}]
}
```

Parameter	Description
`class-list` *name*	Specifies a class list. Entries in the class list map internal IP addresses to IP NAT pools.
`list` *acl-name*	Specifies an Access Control List (ACL) that matches on the inside addresses to be translated. (To configure the ACL, see "access-list (standard)" on page 80 or "access-list (extended)" on page 82.)
`pool` *pool-or-group-name*	Dynamically assigns addresses from a range defined in a pool or pool group.
`static` *inside-ipaddr nat-ipaddr*	Statically maps the specified inside address to a specific NAT address.
`ha-group-id` *group-id*	HA group ID, 1-31.

Default

None

Mode

Configuration mode

Usage

For static NAT mappings, the following limitations apply:

- Application Level Gateway (ALG) services other than FTP are not supported when the server is on the inside.
- HA session synchronization is not supported. However, sessions will not be interrupted by HA failovers.
- Syn-cookies are not supported.

Example

The following command configures static inside NAT translation of 10.10.10.55 to 192.168.20.44:

```
AX(config)#ip nat inside source static 10.10.10.55 192.168.20.44
```

ip nat lsn

Description

Configure Large Scale NAT (LSN) parameters. See “Config Commands: Large Scale NAT” on page 455.

ip nat pcp

Configure Port Control Protocol (PCP). See “Config Commands: Port Control Protocol” on page 505.

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]
[ha-group-id group-id [ha-use-all-ports]]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | */mask-length*}	Network mask for the IP addresses in the pool.
gateway *ipaddr*	Default gateway to use for NATted traffic.
ha-group-id *group-id* [**ha-use-all-ports**]	HA group ID, 1-31. The **ha-use-all-ports** option disables division of the pool’s ports between AX devices. Without this option, the AX device automatically allocates half of each pool address’s ports to one of

the AX devices and allocates the other half of the ports to the other AX device. (See "Usage" below.)

Note: It is recommended to use the **ha-use-all-ports** option only for DNS virtual ports. Using this option with other virtual port types is not valid.

Default None.

Mode Configuration mode

Usage The pool can be used by other **ip nat** commands. The IP addresses must be IPv4 addresses. To configure a pool of IPv6 addresses, see "ipv6 nat pool" on page 270.

To enable inside or outside NAT on interfaces, see "ip nat" on page 214.

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.

For conditions under which the NAT gateway is needed, if no NAT gateway is configured, the AX device uses the default gateway configured for the AX device's other traffic instead.

Port Allocation Between AX Devices in High Availability Deployments (ha-use-all-ports option)

By default, when you assign an IP NAT pool to an HA group, the AX device automatically allocates half of each pool address's ports to one of the AX devices and allocates the other half of the ports to the other AX device.

This automatic allocation is used to prevent simultaneous use of the same port number by both AX devices. For example, without this protection, it would be possible for the same IP address and protocol port number to be in use on both AX devices in an Active-Active configuration.

However, this protection also requires the pool to be configured with more addresses than will actually be needed.

In some cases, there is no benefit to dividing the pool's ports between the AX devices. In particular, there is no benefit for DNS virtual ports. DNS sessions are very short-lived and are never synchronized between the AX devices. For this reason, there is no risk that the same NAT port will be in use on more than one session at the same time. You can use the **ha-use-all-ports** option to disable division of the ports between AX devices.

Note: It is recommended to use the **ha-use-all-ports** option only for DNS virtual ports. Using this option with other virtual port types is not valid.

Example The following command configures an IP address pool named "pool1" that contains addresses from 30.30.30.1 to 30.30.30.254:

```
AX(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
[ha-group-id group-id]
```

Parameter	Description
pool-group-name	Name of the pool group.
ha-group-id *group-id*	HA group ID, 1-31.

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. See "Config Commands: Global" on page 79.)

Parameter	Description
member *pool-name*	Name of a configured IP address pool.

Default None.

Mode Configuration mode

Usage To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

For Large Scale NAT (LSN), a pool group can contain up to 25 pools. For other types of NAT, a pool group can contain up to 5 pools. Pool group members must belong to the same protocol family (IPv4 or IPv6) and must use the same HA ID. A pool can be a member of multiple pool groups.

If a pool group contains pools in different subnets, the AX 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 AX selects the pool that is in the subnet for the outbound route.

The AX 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:

```
AX(config)#ip nat pool-group group1
AX(config-pool-group)member pool1
AX(config-pool-group)member pool2
AX(config-pool-group)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
[vrid {num | default}]
[ha-group-id group-id]
```

Parameter	Description
list-name	Name of the static NAT address range.
local-ipaddr /mask-length	Beginning (lowest) IP address in the range of local addresses.
global-ipaddr /mask-length	Beginning (lowest) IP address in the range of global addresses.

count *number*	Number of addresses to be translated, 1-200000. The range contains a contiguous block of the number of addresses you specify. The block of local addresses starts with the address you specify for *local-ipaddr.* Likewise, the block of global addresses begins with the address you specify for *global-ipaddr.*
ha-group-id *group-id*	HA group ID, 1-31. Specifying the HA group ID allows a newly Active AX device to properly continue management of NATted IP resources following a failover.

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:

```
AX(config)#ip nat range-list nat-list-1 10.10.10.97 /16 192.168.22.50 /16
count 100
```

ip nat reset-idle-tcp-conn

Description Enable client and server TCP Resets for NATted TCP sessions that become idle.

Syntax `[no] ip nat reset-idle-tcp-conn`

Default Disabled.

Mode Configuration mode

ip nat template http-alg

Description Configure a template for HTTP Application Level Gateway (ALG) support. See “ip nat template http-alg” on page 477.

ip nat template logging

Description

Configure a logging template for IPv6 migration features. See “ip nat template logging” on page 593.

ip nat template pcp

Description

Configure a template for Port Control Protocol (PCP). See “ip nat template pcp” on page 506

ip nat translation

Description

Configure NAT timers.

Syntax

```
[no] ip nat translation
{
icmp-timeout {seconds | fast} |
service-timeout {tcp | udp} portnum [to portnum]
  {seconds | fast} |
tcp-timeout seconds |
udp-timeout seconds
}
```

Parameter	Description
`icmp-timeout` *seconds* | `fast`	Specifies how long NATted ICMP sessions can remain idle before being terminated. You can specify 60-15000 seconds, or **fast**. The **fast** option terminates the session as soon as a response is received.
`service-timeout {tcp | udp}` *portnum* `[to` *portnum*`]` `{`*seconds* | `fast}`	Specifies how long 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 60-15000 seconds, or **fast**. The **fast** option terminates the session as soon as a response is received.

`tcp-timeout` *`seconds`*	Timeout for TCP sessions that are not ended normally by a FIN or RST. You can specify 60-15000 seconds, in intervals of 60 seconds.
`udp-timeout` *`seconds`*	Timeout for UDP sessions. You can specify 60-300 seconds, in intervals of 60 seconds.

Default

The NAT timers have the following defaults:

- **icmp-timeout** – SLB maximum session life (MSL), which is 2 seconds by default. (See “slb msl-time” on page 620.)
- **service-timeout** – Not set. For all service ports except UDP 53, the **tcp-timeout** or **udp-timeout** setting is used. For UDP port 53, the SLB MSL time is used.
- **tcp-timeout** – 300 seconds
- **udp-timeout** – 300 seconds

Mode

Configuration mode

Example

The following command changes the SYN timeout to 120 seconds:

```
AX(config)#ip nat translation syn-timeout 120
```

ip prefix-list

Description

Configure an IP prefix list.

Syntax

```
[no] ip prefix-list {name | sequence-num}
[seq sequence-num]
{deny | permit}
{any | ipaddr/mask-length}
[ge prefix-length] [le prefix-length]
```

Parameter	Description
*`name	sequence-num`*	Name or sequence number of the IP prefix-list rule. The name can not contain blanks. The sequence number can be 1-4294967295.
`seq` *`sequence-num`*	Changes the sequence number of the IP prefix-list rule. The sequence number can be 1-4294967295.

deny | permit

Action to take for IP addresses that match the prefix list.

any | *ipaddr /mask-length*

IP address and number of mask bits, from left to right, on which to match. If you omit the **ge** and **le** options (described below), the *mask-length* is also the subnet mask on which to match.

ge *prefix-length*

Specifies a range of prefix lengths on which to match. Any prefix length equal to or greater than the one specified will match. For example, **ge 25** will match on any of the following mask lengths: /25, /26, /27, /28, /29, /30, /31, or /32.

le *prefix-length*

Specifies a range of prefix lengths on which to match. Any prefix length less than or equal to the one specified will match. The lowest prefix length in the range is the prefix specified with the IP address. For example, **192.168.1.0/24 le 28** will match on any of the following mask lengths: /24, /25, /26, /27, or /28.

Default

N/A

Mode

Configuration mode

Usage

You can use IP prefix lists to provide input to certain OSPF, BGP, and RIP routing commands. (For information, see the chapters for each routing protocol.)

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 can not be changed or deleted. If an IP address does not match any of the rules in the IP prefix list, the AX 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 AX 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.

ip prefix-list *list-id* description

Description

Add a description to an IP prefix list.

Syntax

[**no**] **ip prefix-list** {*name* | *sequence-num*} **description** *string*

Parameter	Description
name | *sequence-num*	Name or sequence number of the IP prefix-list rule.
description *string*	Description of the IP prefix list. The string can be up to 80 characters, and can contain blanks. Quotation marks are not required.

Default

None

Mode

Configuration mode

Usage

The description is placed above the rule it describes. (See the CLI example.)

Example

The following commands add descriptions to some IP prefix-list rule and display the results:

```
AX(config)#ip prefix-list aaa description Here is a string to describe the
rule.
AX(config)#ip prefix-list ccc description And here is a string to describe this
rule.
AX(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 prefix-list sequence-number

Description Enable or disable display of the sequence numbers of IP prefix-list rules.

Syntax

```
[no] ip prefix-list sequence-number
```

Default Enabled

Mode Configuration mode

Usage When this option is enabled, the sequence numbers are displayed in the running-config. After you save the configuration, the sequence numbers also are displayed in the startup-config.

Example The following commands configure some IP prefix-list rules, then display them in the running-config. Display of sequence numbers is enabled.

```
AX(config)#ip prefix-list aaa deny 10.10.10.0/8 le 24
AX(config)#ip prefix-list bbb permit 192.168.1.0/24
AX(config)#ip prefix-list ccc permit any
AX(config)#show running-config | section ip prefix-list
ip prefix-list aaa seq 5 permit any
ip prefix-list bbb seq 10 permit 192.168.1.0/24
ip prefix-list ccc seq 15 deny 10.10.10.0/8 le 24
```

Example The following commands disable display of sequence numbers, then re-display the IP prefix-list rules:

```
AX(config)#no ip prefix-list sequence-number
AX(config)#show running-config | section ip prefix-list
ip prefix-list aaa deny 10.10.10.0/8 le 24
ip prefix-list bbb permit 192.168.1.0/24
ip prefix-list ccc permit any
```

ip route

Description Configure a static IP route.

Syntax

```
[no] ip route destination-ipaddr
{subnet-mask | /mask-length}
next-hop-ipaddr
[distance]
[cpu-process]
```

Parameter	Description
destination-ipaddr {subnet-mask | /mask-length}	Specifies the destination of the route. To configure a default route, specify 0.0.0.0/0.
next-hop-ipaddr	Specifies the next-hop router to use to reach the route destination. The address must be in the same subnet as the AX Series device.
distance	Distance value for the route, 1-255.
cpu-process	Sends traffic that uses this route to the CPU for processing. This option is applicable only to models AX 2200, AX 3100, AX 3200, AX 5100, and AX 5200. The option does not appear in the CLI on other models.

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).

Example

The following command configures a default route using gateway 10.10.10.1 and the default metric:

```
AX(config)#ip route 0.0.0.0/0 10.10.10.1
```

ip stateful-firewall

Description

Configure the AX device to perform some of the basic functions of a stateful firewall for transparent Layer 3 traffic. Traffic originating from an external device is filtered using an ACL or based on the state information of an existing ALG session.

Syntax

```
[no] ip stateful-firewall
{
alg {options}
{disable | enable | rtp-stun-timeout} |
disable |
enable |
endpoint-independent-filtering |
ha-group-id |
stun-timeout |
tcp |
udp
}
```

Parameter	Description
alg *{options}* **{disable | enable | rtp-stun-timeout}**	Enable or disable stateful firewall support for specific ALG protocols. *Options* refers to the following ALG protocols: **ftp**, **tftp**, **rtsp**, **pptp**, **sip** The **rtp-stun-timeout** option configures the STUN timeout for EIF sessions.
disable	Disable stateful firewall on a global basis.
enable	Enable stateful firewall on a global basis.
[no] endpoint-independent-filtering {tcp | udp} {enable | disable} [ephemeral | well-known | *port-num* **[to** *port-num***]]**	Configure filtering behavior for stateful firewall. Enable or disable EIF for ephemeral, well-known, or a range of ports. The **ephemeral**

option enables or enables EIF on ports 1024-65535. The **well-known** option enables or disables EIF on ports 1-1023. The **tcp** and **udp** *port-num* **to** *port-num* options enable or disable EIF on a specific port or on ports 1-65535.

ha-group-id

Configure a High Availability Group ID for stateful firewall.

stun-timeout

Configure the STUN timeout for endpoint-independent filtering. Configure the Session Traversal Utilities for NAT (STUN) timeout. Number is specified in minutes for EIF, and it can range from 0-60 minutes. The default is 2 minutes.

[**no**] **tcp** {**idle-timeout** | **stun-timeout** | **syn-timeout**} [**port** *portnum* [**to** *portnum*]] *seconds*

Configure TCP parameters for stateful firewall. The **idle-timeout** option allows you to specify the number of seconds a stateful firewall session can remain idle before the AX device terminates the session. You can specify 60-15000 seconds. The default is 300 seconds.

The **stun-timeout** option allows you to specify the number of minutes for EIF. You can specify 0-60 minutes. The default is 2 minutes.

The **syn-timeout** option allows you to specify the amount of time the session stays alive before the TCP handshake is completed and the session is established. You can specify 2-30 seconds. The default is 4 seconds. (The second session can remain in a half-open state before being deleted.).

[**no**] **udp** {**idle-timeout** | **stun-timeout**} [**port** *portnum* [**to** *portnum*]] *seconds*

Configure UDP parameters for stateful firewall. See **idle** and **stun timeout** option descriptions for **tcp** above.

Default Disabled on a global basis. See parameter descriptions above for specific default values, where applicable.

Introduced in Release 2.6.6-P4

Mode Configuration mode

Usage Stateful firewall support for transparent sessions enables the AX device to provide basic functions of a stateful firewall. The stateful firewall feature protects internal users with public IPs from external attacks through the use of access control lists, which deny or reject traffic from unrecognized external sources. The AX device maintains state information for Application Layer Gateway protocol traffic, which can originate from either side of the firewall, enabling that traffic to pass through the firewall unimpeded.

You can enable stateful firewall support for the following ALG protocols:

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Real Time Streaming Protocol (RTSP)
- Point-to-Point Tunneling Protocol (PPTP)* Generic Routing Encapsulation (GRE)
- Session Initiation Protocol (SIP)

Note: If you enable stateful firewall support without specifying a particular port, then endpoint-independent filtering (EIF) is enabled on all ports (1-65535).

Example The following example globally enables the stateful firewall feature and sets up the access list. An inside stateful firewall is enabled on private VE port 21, and an outside stateful firewall is enabled on public VE port 22, and access list “101” is applied.

```
AX(config)#ip stateful-firewall enable
AX(config)#access-list 101 permit tcp any any log
AX(config)#access-list 101 permit udp any any log
AX(config)#interface ve 21
AX(config-if:ve21)#ip address 10.10.10.33 255.255.255.0
AX(config-if:ve21)#ip stateful-firewall inside
AX(config)#interface ve 22
AX(config-if:ve22)#ip address 20.20.20.33 255.255.255.0
AX(config-if:ve22)#ip stateful-firewall outside access-list 101
```

*. PPTP has not been tested in the 2.6.6-P4 release.

```
AX(config-if:ve22)#exit
```

Config Commands: IPv6

The IPv6 commands configure global IPv6 parameters.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Note: To configure global IPv4 parameters, see “Config Commands: IP” on page 239.

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}

{any | host host-src-ipv6addr |
  net-src-ipv6addr /mask-length}

{any | host host-dst-ipv6addr |
  net-dst-ipv6addr /mask-length}

[fragments] [vlan vlan-id] [dscp num]

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

or

Syntax

```
[no] {permit | deny} {tcp | udp}

{any | host host-src-ipv6addr |
  net-src-ipv6addr /mask-length}
  [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}
  [eq dst-port | gt dst-port | lt dst-port |
  range start-dst-port end-dst-port]

[fragments] [vlan vlan-id] [dscp num]
  [established]

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

Parameter	Description
seq-num	Sequence number of this rule in the ACL. You can use this option to resequence the rules in the ACL.
deny | **permit**	Action to take for traffic that matches the ACL. **deny** – Drops the traffic. **permit** – Allows the traffic.
ipv6 | **icmp**	Filters on IPv6 or ICMP packets.
tcp | **udp**	Filters on TCP or UDP packets. The **tcp** and **udp** options enable you to filter on protocol port numbers.
any | **host** *host-src-ipv6addr* | *net-src-ipv6addr /mask-length*	Source IP address(es) to filter. **any** – The ACL matches on all source IP addresses. **host** *host-src-ipv6addr* – The ACL matches only on the specified host IPv6 address. *net-src-ipv6addr /mask-length* – The ACL matches on any host in the specified subnet. The *mask-length* specifies the portion of the address to filter.
eq *src-port* | **gt** *src-port* | **lt** *src-port* | **range** *start-src-port end-src-port*	For **tcp** or **udp**, the source protocol ports to filter. **eq** *src-port* – The ACL matches on traffic from the specified source port. **gt** *src-port* – The ACL matches on traffic from any source port with a higher number than the specified port. **lt** *src-port* – The ACL matches on traffic from any source port with a lower number than the specified port.

	range *start-src-port end-src-port* – The ACL matches on traffic from any source port within the specified range.
any | **host** *host-dst-ipv6addr* | *net-dst-ipv6addr /mask-length*	Destination IP address(es) to filter.
eq *dst-port* | **gt** *dst-port* | **lt** *dst-port* | **range** *start-dst-port end-dst-port*	For **tcp** or **udp**, the destination protocol ports to filter.
fragments	Matches on packets in which the More bit in the header is set (1) or has a non-zero offset.
vlan *vlan-id*	Matches on the specified VLAN. VLAN matching occurs for incoming traffic only.
dscp *num*	Matches on the 6-bit Diffserv value in the IP header, 1-63.
established	Matches on TCP packets in which the ACK or RST bit is not set. This option is useful for protecting against attacks from outside. Since a TCP connection from the outside does not have the ACK bit set (SYN only), the connection is dropped. Similarly, a connection established from the inside always has the ACK bit set. (The first packet to the network from outside is a SYN/ACK.)
log [**transparent-session-only**]	Configures the AX 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.

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 frag timeout

Description Configure the timeout for IPv6 packet fragments.

Syntax

```
[no] ipv6 frag timeout ms
```

Parameter	Description
ms	Specifies the number of milliseconds (ms) the AX 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 4-16000 ms, in 10-ms increments.

Default 1000 ms (1 second)

Mode Configuration mode

ipv6 icmpv6 disable

Description Disable ICMPv6 messages.

Syntax

```
[no] ipv6 icmpv6 disable {redirect | unreachable}
```

Parameter	Description
redirect.	Disables sending of ICMPv6 Redirect messages.
unreachable.	Disables sending of ICMPv6 Destination Unreachable messages.

Default Both types of ICMP messages are enabled.

Mode Configuration mode

Usage The following command disables sending of IPv6 ICMP Destination Unreachable messages:

```
AX(config)#ipv6 icmpv6 disable unreachable
```

ipv6 nat icmpv6

Description Enable ping replies from NAT pool addresses.

Syntax

```
[no] ipv6 nat icmpv6 respond-to-ping
```

Default By default, the AX device does not reply to ping requests that are sent to NAT addresses (LSN NAT pool addresses). Instead, by default, the AX device drops ping requests sent to LSN NAT pool addresses.

Introduced in Release 2.6.6-P6

Mode Configuration mode

ipv6 nat inside

Description Enable inside NAT on the interface.

Syntax

```
[no] ipv6 nat inside
```

Default Disabled

Mode Configuration mode

ipv6 nat pool

Description Configure a named set of IPv6 addresses for use by NAT.

Syntax

```
[no] ipv6 nat pool pool-name
start-ipv6-addr end-ipv6-addr
netmask mask-length
[lsn [max-users-per-ip num]]
[gateway ipaddr]
[ha-group-id group-id]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.

end-ipaddr	Ending (highest) IP address in the range.
netmask *mask-length*	Network mask for the IP addresses in the pool, 64-128.
lsn [**max-users-per-ip** *num*]	Enables the pool to be used for Large Scale NAT (LSN). The **max-user-per-ip** option specifies the maximum number of internal addresses that can be mapped to a single public address at the same time. You can specify 1-65535. By default, there is no limit.
gateway *ipv6-addr*	Next-hop gateway address.
ha-group-id *group-id*	HA group ID, 1-31.

Default None.

Mode Configuration mode

Example The following command configures an IPv6 address pool named “ipv6pool2”:

```
AX(config)#ipv6 nat pool ipv6pool2 abc1::1 abc1::10 netmask 96
```

ipv6 neighbor

Description Configure a static IPv6 neighbor.

Syntax

```
[no] ipv6 neighbor ipv6-addr macaddr
ethernet port-num [vlan vlan-id]
```

Parameter	Description
ipv6-addr	IPv6 unicast address of the neighbor.
macaddr	MAC address of the IPv6 neighbor.
port-num	Ethernet interface connected to the neighbor.
vlan-id	VLAN for which to add the IPv6 neighbor entry. If you do not specify the VLAN, the entry is added for all VLANs.

Default N/A

Mode Configuration mode

Usage The neighbor must be directly connected to the AX Series device's Ethernet port you specify, or connected through a Layer 2 switch.

Example The following command configures IPv6 neighbor 2001:db8::1111:2222 with MAC address abab.cdcd.efef, connected to the AX Series device's Ethernet port 5:

```
AX(config)#ipv6 neighbor 2001:db8::1111:2222 abab.cdcd.efef ethernet 5
```

ipv6 ospf display

Description Change how IPv6 routes are displayed in **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 pmtu {disable | enable}

Description

Please contact A10 Networks for information.

Syntax

```
[no] ipv6 pmtu {disable | enable}
```

ipv6 pmtu timeout

Description

Please contact A10 Networks for information.

Syntax

```
[no] ipv6 pmtu timeout seconds
```

ipv6 prefix-list

Description

Configure an IPv6 prefix list.

Syntax

```
[no] ipv6 prefix-list {name | sequence-num}
[seq sequence-num]
{deny | permit}
{any | ipaddr/mask-length}
[ge prefix-length] [le prefix-length]
```

Parameter	Description
name | *sequence-num*	Name or sequence number of the IP prefix-list rule. The name can not contain blanks. The sequence number can be 1-4294967295.
seq *sequence-num*	Changes the sequence number of the IP prefix-list rule. The sequence number can be 1-4294967295.
deny | **permit**	Action to take for IP addresses that match the prefix list.
any | *ipv6addr /mask-length*	IPv6 address and number of mask bits, from left to right, on which to match. If you omit the **ge** and **le** options (described below), the *mask-length* is also the subnet mask on which to match.

ge *prefix-length*

Specifies a range of prefix lengths on which to match. Any prefix length equal to or greater than the one specified will match. For example, **ge 25** will match on any of the following mask lengths: /25, /26, /27, /28, /29, /30, /31, or /32.

le *prefix-length*

Specifies a range of prefix lengths on which to match. Any prefix length less than or equal to the one specified will match. The lowest prefix length in the range is the prefix specified with the IP address. For example, **192.168.1.0/24 le 28** will match on any of the following mask lengths: /24, /25, /26, /27, or /28.

Default

N/A

Mode

Configuration mode

Usage

You can use IP prefix lists to provide input to certain OSPF, BGP, and RIP routing commands. (For information, see the chapters for each routing protocol.)

How Matching Occurs

Matching begins with the lowest numbered IPv6 prefix-list rule and continues until the first match is found. The action in the first matching rule is applied to the IPv6 address.

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 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.

Implied Deny any Rule

The IPv6 prefix list has an implied **deny any** rule at the end. This rule is not visible and can not be changed or deleted. If an IPv6 address does not match any of the rules in the IPv6 prefix list, the AX device uses the implied **deny any** rule to deny the address.

Sequence Numbering

As described above, the sequence of rules in the IPv6 prefix list can affect whether a given address matches a permit rule or a deny rule.

When you configure the first IPv6 prefix-list rule, the AX 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.

ipv6 prefix-list *list-id* description

Description Add a description to an IPv6 prefix list.

Syntax

```
[no] ipv6 prefix-list {name | sequence-num}
description string
```

Parameter	Description
name | *sequence-num*	Name or sequence number of the IPv6 prefix-list rule.
description *string*	Description of the IPv6 prefix list. The string can be up to 80 characters, and can contain blanks. Quotation marks are not required.

Default None

Mode Configuration mode

Usage The description is placed above the rule it describes.

ipv6 prefix-list sequence-number

Description Enable or disable display of the sequence numbers of IPv6 prefix-list rules.

Syntax

```
[no] ipv6 prefix-list sequence-number
```

Default Enabled

Mode Configuration mode

Usage When this option is enabled, the sequence numbers are displayed in the running-config. After you save the configuration, the sequence numbers also are displayed in the startup-config.

ipv6 route

Description Configure a static IPv6 route.

Syntax

```
[no] ipv6 route ipv6-addr/prefix-length
gateway-addr
[distance]
```

Parameter	Description
ipv6-addr	IPv6 unicast address of the route destination.
prefix-length	Prefix length, 1-128.
gateway-addr	IPv6 unicast address of the next-hop gateway to the destination.
distance	Distance value for the route, 1-255.

Default N/A

Mode Configuration mode

Usage The **ethernet**, **trunk**, and **ve** options are available only if the *gateway-addr* 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 can not be a member of a trunk or a VE. If you use a trunk, the trunk can not be a member of a VE.
- After you configure the static route, you can not 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.

Example The following command configures a static IPv6 route to destination 2001:db8::3333:3333/32, though gateway 2001:db8::3333:4444:

```
AX(config)#ipv6 route 2001:db8::3333:3333/32 2001:db8::3333:4444
```

Example The following command configures a default IPv6 route:

```
AX(config)#ipv6 route ::/0 abc1::1111
```

The following command configures an IPv6 static route that uses Ethernet port 6’s link-local address as the next hop:

```
AX(config)#ipv6 route abaa:3::0/64 fe80::2 ethernet 6
```

ipv6 stateful firewall

Description See “ip stateful-firewall” on page 260.

Introduced in Release 2.6.6-P4

Config Commands: Router – RIP

This chapter describes the syntax for the Routing Information Protocol (RIP) commands in AX Release 2.6.6. The commands are described in the following sections:

- "Enabling RIP" on page 279
- "IPv4 RIP Configuration Commands" on page 281
- "IPv6 RIP Configuration Commands" on page 296
- "RIP Show Commands" on page 308
- "RIP Clear Commands" on page 308

Note: This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See "clear" on page 59.
- **debug** – See "debug" on page 64.
- **do** – See "do" on page 117.
- **end** – See "end" on page 123.
- **exit** – See "exit" on page 124.
- **no** – See "no" on page 155.
- **show** – See "Show Commands" on page 689.
- **write** – See "write terminal" on page 78.

Enabling RIP

You can enable RIP for IPv4 and RIP for IPv6. Each version runs independently of the other. The AX device supports a single IPv4 RIP process and a single IPv6 RIP process.

Note: Optionally you also can enable RIPv1. RIPv1 and RIPv2 can be enabled separately for inbound and outbound RIP traffic.

Enabling RIP for IPv4

1. To enable the protocol and access the configuration level for global IPv4 RIP parameters, enter the following command at the global configuration level:

   ```
   router rip
   ```

2. To enable IPv4 RIP for specific networks, enter the following command separately for each network:

   ```
   network {ipaddr/mask-length | interface}
   ```

This is the minimum required configuration. Additional configuration may be required depending on your deployment.

Enabling RIP for IPv6

1. To enable the protocol and access the configuration level for global IPv6 RIP parameters, enter the following command at the global configuration level:

   ```
   router ipv6 rip
   ```

2. To enable IPv6 RIP on an individual interface:

   a. Use the following command to return to the global configuration level of the CLI:

   ```
   exit
   ```

   b. Use the following command to access the interface:

   ```
   interface
   {ethernet port-num | ve ve-num |
   loopback num | management | trunk num}
   ```

   c. Use the following command to enable IPv6 RIP on the interface:

   ```
   ipv6 router rip
   ```

This is the minimum required configuration. Additional configuration may be required depending on your deployment.

IPv4 RIP Configuration Commands

The configuration commands in the following sections are applicable to IPv4 RIP.

- "Global IPv4 RIP Commands" on page 281
- "Interface-Level IPv4 RIP Commands" on page 293

Global IPv4 RIP Commands

The commands in this section apply globally to the IPv4 RIP process.

To access the configuration level for the IPv4 RIP process, use the **router rip** command at the global configuration level of the CLI.

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 AX device).
disable	The metric values displayed for routes in the RIP routing table are the values ***after*** modification by this RIP router (the AX 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
```

Parameter	Description
num	Specifies the default metric, 1-16.

Default 1

Mode IPv4 RIP

distance

Description Set the administrative distance for IPv4 RIP routes.

Syntax

```
[no] distance num [ipaddr/mask-length [acl-id]]
```

Parameter	Description
num	Administrative distance, 1-255.
ipaddr/mask-length	Network prefix and mask length. The specified distance is applied only to routes with a matching source address.
acl-id	ACL ID. The specified distance is applied only to routes that match the source IP address in the ACL.

Note: In the ACL, use the **permit** action, not the **deny** action.

Default The default distance is 120.

Mode IPv4 RIP

Usage The administrative distance specifies the trustworthiness of routes. In cases where there are multiple routes to the same destination, from different routing protocols, the administrative distance can be used as a tie-breaker.

A low administrative distance value indicates a high level of trust. Likewise, a high administrative distance value indicates a low level of trust. For example, setting the administrative distance value for external routes to 255 means those routes are very untrustworthy and should not be used.

distribute-list

Description

Configure filtering of route updates.

Syntax

```
[no] distribute-list {acl-id | prefix list-name}
{in | out} [interface]
```

Parameter	Description
acl-id | **prefix** *list-name*	ACL or prefix list that specifies the routes to filter. The action you use in the ACL or prefix list determines whether matching routes are allowed: **permit** – Matching routes are allowed. **deny** – Matching routes are prohibited.
in | **out**	Traffic direction for which to filter updates: **in** – Inbound route updates are filtered. **out** – Outbound route updates are filtered.
interface	Interface on which updates are filtered. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface. **loopback** [*num*] – Loopback interface. If you do not specify an interface number, route updates are filtered out on all loopback interfaces. **management** – Ethernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface. If you do not specify an interface, 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 AX 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:

```
AX(config)#ip prefix-list rip-subnet-only permit 30.30.30.0/24
AX(config)#router rip
AX(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:

```
AX(config)#access-list 23 permit 10.0.0.0 0.255.255.255
AX(config)#router rip
AX(config-router)#distribute-list 23 out ve 45
```

maximum-prefix

Description

Specify the maximum number of routes allowed in the IPv4 RIP route table.

Syntax

```
[no] maximum-prefix num [threshold]
```

Parameter	Description
num	Maximum number of RIP routes allowed. You can specify 1-2048.
threshold	Percentage of the maximum number of routes at which a warning is generated. You can specify 1-100. The warnings appear in the routing log.

Default 256. The default threshold is 75 percent.

Mode IPv4 RIP

neighbor

Description Specify a neighboring IPv4 RIP router.

Syntax

```
[no] neighbor ipaddr
```

Parameter	Description
ipaddr	IP address of the neighboring IPv4 RIP router.

Default None

Mode IPv4 RIP

Usage Enter the command separately for each IPv4 RIP neighbor.

network

Description Enable IPv4 RIP on a network.

Syntax

```
[no] network {ipaddr/mask-length | interface}
```

Parameter	Description
ipaddr/mask-length	Prefix and mask length of a IPv4 RIP network.
interface	Interface on which to enable RIP. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface.

	loopback [*num*] – Loopback interface. If you do not specify an interface number, RIP is enabled on all loopback interfaces. **management** – Ethernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface. If you do not specify an interface, RIP is enabled on all the interfaces.

Note: The **internal** option is not applicable.

Default None

Mode IPv4 RIP

offset-list

Description Increase the metric for specific routes.

Syntax

```
[no] offset-list acl-id {in | out} offset
[interface]
```

Parameter	Description
acl-id	ACL that matches on the routes for which to increase the metric.
in | **out**	Direction to which to apply the metric: **in** – Applies the additional metric value to routes received in updates from RIP neighbors. **out** – Applies the additional metric value to routes advertised to RIP neighbors.
offset	Additional metric to add to routes. You can specify 0-16.
interface	Interface on which to increase the metric. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface. **loopback** [*num*] – Loopback interface. If you do not specify an interface number, the metric is increased on all loopback interfaces.

	management – Etrhernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface. If you do not specify an interface, the metric is increased on all interfaces.

Note: The **internal** option is not applicable.

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 updates from being sent on an interface.

Syntax

```
[no] passive-interface interface
```

Parameter	Description
interface	Interface on which to block RIP updates. 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 updates are blocked on all loopback interfaces. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface.

Default

None. RIP updates 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
```

Parameter	Description
bytes	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 [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. For *options*, see the end of this parameter list.
connected [*options*]	Redistributes route information for directly connected networks into RIP. For *options*, see the end of this parameter list.
floating-ip [*options*]	Redistributes route information for floating IP addresses into RIP. For *options*, see the end of this parameter list.
ip-nat [*options*]	Redistributes routes into RIP for reaching translated NAT addresses allocated from a pool. For *options*, see the end of this parameter list.

ip-nat-list [*options*]
Redistributes routes into RIP for reaching translated NAT addresses allocated from a range list. For *options*, see the end of this parameter list.

isis [*options*]
Redistributes route information from Intermediate System to Intermediate System (IS-IS) into RIP. For *options*, see the end of this parameter list.

ospf [*options*]
Redistributes route information from Open Shortest Path First (OSPF) into RIP. For *options*, see the end of this parameter list.

static [*options*]
Redistributes routes into RIP for reaching networks through static routes. For *options*, see the end of this parameter list.

vip [**only-flagged** | **only-not-flagged** [*options*]]
Redistributes routes into RIP for reaching virtual server IP addresses.

By default, all VIPs are redistributed when you use the **vip** option. To restrict redistribution to a subset of VIPs, use one of the following options:

> **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used.
>
> **only-not-flagged** – Redistributes all VIPs *except* those on which the **redistribution-flagged** command is used.
>
> For more information, see “Usage”.

For *options*, see below.

options
Optional parameters supported for all 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. (To configure a route map, use the **route-map** *map-name* command at the global configuration level of the CLI.)

Note: The **kernel** option is not applicable.

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. For example, if you use the **vip** option, routes to all VIPs are redistributed into RIP.

VIP Redistribution

You can exclude redistribution of individual VIPs using one or the other of the following methods. They are mutually exclusive.

- 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 only-not-flagged** command is automatically converted into the **redistribute vip** command. When you display the configuration, it will contain the **redistribute vip** command, not the **redistribute vip only-not-flagged** command. This command conversion makes the behavior in the current release backwards compatible with the behavior in previous releases.

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:

```
AX(config-router)#redistribute floating-ip
AX(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.

```
AX(config)#slb virtual-server vip1
AX(config-slb virtual server)#redistribution-flagged
AX(config-slb virtual server)#exit
AX(config)#router rip
AX(config-router)redistribute vip only-flagged
```

route

Description

Configure static RIP routes.

Syntax

```
[no] route ipaddr/prefix-length
```

Parameter	Description
ipaddr/prefix-length	Destination of the route.

Default

None

Mode

IPv4 RIP

timers

Description

Configure RIP timers.

Syntax

```
[no] timers basic update timeout
garbage-collection
```

Parameter	Description
update	Amount of time between transmission of RIP route updates to neighbors. You can specify 5-2147483647 seconds.

timeout	Maximum number of seconds the AX 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.)
garbage-collection	Amount of time after a route becomes invalid that the route remains in the route table before being removed. You can specify 5-2147483647 seconds.

Default The RIP timers have the following default values:

- *update* – 30
- *timeout* – 180
- *garbage-collection* – 120

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 AX device.

Caution: RIPv1 is less secure than RIPv2. It is recommended to run RIPv2 if your other routers support it.

Interface-Level IPv4 RIP Commands

The commands in this section apply specifically to the IPv4 interface on which you enter them. In cases where the same parameter can be set globally and on individual interfaces, the setting on an individual interface overrides the global setting.

ip rip authentication

Description

Configure IPv4 RIP authentication on the interface.

Syntax

```
[no] ip rip authentication
{
key-chain name [name ...] |
mode {md5 | text} |
string auth-string [auth-string ...]
}
```

Parameter	Description
key-chain *name* [*name* ...]	Enables authentication using the specified key chains. (To configure a key-chain file, use the **key chain** command at the global configuration level of the CLI.)
mode {**md5** | **text**}	Authentication mode: **md5** – Message Digest 5 **text** – Clear text
string *auth-string* [*auth-string* ...]	Enables authentication using the specified passwords.

Default

None

Mode

Interface

ip rip receive version

Description Specify the RIP version allowed in RIP packets received on the interface.

Syntax

```
[no] ip rip receive version {1 [2] | 2}
```

Parameter	Description
1	RIP version 1.
2	RIP version 2.

Default 2

Mode Interface

ip rip receive-packet

Description Enable the interface to receive RIP packets.

Syntax

```
[no] ip rip receive-packet
```

Default Enabled

Mode Interface

ip rip send version

Description Specify the RIP version allowed to be sent on the interface.

Syntax

```
[no] ip rip send version {1 [2] | 2}
```

Parameter	Description
1	RIP version 1.
2	RIP version 2.

Default 2

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 AX device from advertising a route to the neighbor that advertised the same route to the AX device.

Syntax

```
[no] ip rip split-horizon [poisoned]
```

Parameter	Description
`poisoned`	Enables advertisement of a route to the neighbor that advertised the route to the AX device, but sets the metric value to infinity, thus making the route advertised by the AX device unusable by the neighbor. If you omit the **poisoned** option, advertisement of a route to the neighbor that advertised the route to the AX device is not allowed.

Default Split-horizon with poison is enabled.

Mode Interface

IPv6 RIP Configuration Commands

The configuration commands in the following sections are applicable to IPv6 RIP.

- “Global IPv6 RIP Commands” on page 296
- “Interface-Level IPv6 RIP Command” on page 307

Global IPv6 RIP Commands

The commands in this section apply globally to the IPv6 RIP process.

To access the configuration level for a IPv6 RIP process, use the **router ipv6 rip** command at the global configuration level of the CLI.

aggregate-address

Description Configure an aggregate of multiple IPv6 RIP routes.

Syntax

```
[no] aggregate-address ipv6addr/mask-length
```

Parameter	Description
ipv6addr/mask-length	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 AX device).
disable	The metric values displayed for routes in the RIP routing table are the values ***after*** modification by this RIP router (the AX 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
```

Parameter	Description
num	Specifies the default metric, 1-16.

Default 1

Mode IPv6 RIP

distribute-list

Description Configure filtering of route updates.

Syntax

```
[no] distribute-list {acl-id | prefix list-name}
{in | out} [interface]
```

Parameter	Description
acl-id | **prefix** *list-name*	ACL or prefix list that specifies the routes to filter. The action you use in the ACL or prefix list determines whether matching routes are allowed: **permit** – Matching routes are allowed. **deny** – Matching routes are prohibited.
in | **out**	Traffic direction for which to filter updates: **in** – Inbound route updates are filtered. **out** – Outbound route updates are filtered.
interface	Interface on which updates are filtered. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface. **loopback** [*num*] – Loopback interface. If you do not specify an interface number, route updates are filtered out on all loopback interfaces. **management** – Ethernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface. If you do not specify an interface, the filter applies to all interfaces.

Note: The **internal** option is not applicable.

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 AX device can have one global inbound distribute list and one global outbound distribute list. Likewise, each interface can have one inbound distribute list and one outbound distribute list.

For inbound updates, if the interface on which the update is received has a distribute list, that distribute list is checked before the global distribute list. Likewise, for outbound updates, the distribute list on the outbound interface is checked before the global distribute list. The action (permit or deny) in the first distribute list that matches is used.

ACL Implicit Deny Rule

Every ACL has an implicit "deny any" rule at the end. Traffic that does not match any of the explicitly configured rules in an ACL will match the implicit deny rule.

neighbor

Description Specify a neighboring IPv6 RIP router.

Syntax `[no] neighbor ipv6addr interface`

Parameter	Description
ipv6addr	Link-local IPv6 address of the neighboring IPv6 RIP router.
interface	Interface on which the neighbor can be reached. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface. **loopback** [*num*] – Loopback interface. If you do not specify an interface number, the neighbor is added for all loopback interfaces. **management** – Etrhernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface.

Note: The **internal** option is not applicable.

Default None

Mode IPv6 RIP

Usage Enter the command separately for each IPv4 RIP neighbor.

offset-list

Description Increase the metric for specific routes.

Syntax

```
[no] offset-list acl-id {in | out} offset
[interface]
```

Parameter	Description
acl-id	ACL that matches on the routes for which to increase the metric.
in | out	Direction to which to apply the metric: **in** – Applies the additional metric value to routes received in updates from RIP neighbors. **out** – Applies the additional metric value to routes advertised to RIP neighbors.
offset	Additional metric to add to routes. You can specify 0-16.
interface	Interface on which to increase the metric. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface. **loopback** [*num*] – Loopback interface. If you do not specify an interface number, the metric is increased on all loopback interfaces. **management** – Etrhernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface. If you do not specify an interface, the metric is increased on all interfaces.

Note: The **internal** option is not applicable.

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
```

Parameter	Description
interface	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
```

Parameter	Description
bytes	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. For *options*, see the end of this parameter list.
connected [*options*]	Redistributes route information for directly connected networks into RIP. For *options*, see the end of this parameter list.
floating-ip [*options*]	Redistributes route information for floating IP addresses into RIP. For *options*, see the end of this parameter list.
ip-nat [*options*]	Redistributes routes into RIP for reaching translated NAT addresses allocated from a pool. For *options*, see the end of this parameter list.
ip-nat-list [*options*]	Redistributes routes into RIP for reaching translated NAT addresses allocated from a range list. For *options*, see the end of this parameter list.
isis [*options*]	Redistributes route information from Intermediate System to Intermediate System (IS-IS) into RIP. For *options*, see the end of this parameter list.
ospf [*options*]	For *options*, see the end of this parameter list.

static [*options*]

Redistributes routes into RIP for reaching networks through static routes. For *options*, see the end of this parameter list.

vip [**only-flagged** | **only-not-flagged** [*options*]]

Redistributes routes into RIP for reaching virtual server IP addresses.

By default, all VIPs are redistributed when you use the **vip** option. To restrict redistribution to a subset of VIPs, use one of the following options:

> **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used.
>
> **only-not-flagged** – Redistributes all VIPs *except* those on which the **redistribution-flagged** command is used.
>
> For more information, see “Usage”.

For *options*, see below.

options

Optional parameters supported for all 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. (To configure a route map, use the **route-map** *map-name* command at the global configuration level of the CLI.)

Note: The **kernel** option is not applicable.

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. For example, if you use the **vip** option, routes to all VIPs are redistributed into RIP.

VIP Redistribution

You can exclude redistribution of individual VIPs using one or the other of the following methods. They are mutually exclusive.

- 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 only-not-flagged** command is automatically converted into the **redistribute vip** command. When you display the configuration, it will contain the **redistribute vip** command, not the **redistribute vip only-not-flagged** command. This command conversion makes the behavior in the current release backwards compatible with the behavior in previous releases.

VIP Redistribution Usage Examples:

- If you have 10 VIPs and all of them need to be redistributed by RIP, use the **redistribute vip** command at the configuration level for the RIP process.
- If you have 10 VIPs but only 2 of them need to be redistributed, use the **redistribution-flagged** command at the configuration level for each of the 2 VIPs, then use the **redistribute vip only-flagged** command at the configuration level for the RIP process.
- If you have 10 VIPs and need to redistribute 8 of them, use the **redistribution-flagged** command at the configuration level for the 2 VIPs that should *not* be redistributed. Enter the **redistribute vip only-not-flagged** command at the configuration level for the RIP process. (In this case, alternatively, you could enter **redistribute vip** instead of **redistribute vip only-not-flagged**.)

route

Description Configure static RIP routes.

Syntax

```
[no] route ipv6addr/prefix-length
```

Parameter	Description
ipv6addr/ prefix-length	Destination of the route.

Default None

Mode IPv6 RIP

route-map

Description Configure a list of interfaces to use as input to other RIP commands.

Syntax

```
[no] route-map map-name {in | out} interface
```

Parameter	Description
map-name	Name of the route map.
in | out	Direction to which the map applies: **in** – Applies to incoming routes received in updates from RIP neighbors. **out** – Applies to routes advertised to RIP neighbors.
interface	Interface to which to apply the route map. You can specify the following types of interfaces: **ethernet** *portnum* – Ethernet data interface. **loopback** [*num*] – Loopback interface. If you do not specify an interface number, the route map is applied to all loopback interfaces. **management** – Etrhernet management interface. **trunk** *trunknum* – Trunk interface. **ve** *ve-num* – Virtual Ethernet (VE) interface.

Default None

Mode IPv6 RIP

timers

Description Configure RIP timers.

Syntax

```
[no] timers basic update timeout
garbage-collection
```

Parameter	Description
update	Amount of time between transmission of RIP route updates to neighbors. You can specify 5-2147483647 seconds.
timeout	Maximum number of seconds the AX 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.)
garbage-collection	Amount of time after a route becomes invalid that the route remains in the route table before being removed. You can specify 5-2147483647 seconds.

Default The RIP timers have the following default values:

- *update* – 30
- *timeout* – 180
- *garbage-collection* – 120

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.

Interface-Level IPv6 RIP Command

The commands in this section apply specifically to the IPv6 interface on which you enter them. In cases where the same parameter can be set globally and on individual interfaces, the setting on an individual interface overrides the global setting.

ipv6 rip split-horizon

Description

Configure the split-horizon method. Split horizon prevents the AX device from advertising a route to the neighbor that advertised the same route to the AX device.

Syntax

```
[no] ipv6 rip split-horizon [poisoned]
```

Parameter	Description
poisoned	Enables advertisement of a route to the neighbor that advertised the route to the AX device, but sets the metric value to infinity, thus making the route advertised by the AX device unusable by the neighbor. If you omit the **poisoned** option, advertisement of a route to the neighbor that advertised the route to the AX device is not allowed.

Default

Split-horizon with poison is enabled.

Mode

Interface

RIP Show Commands

This section lists the RIP show commands.

show ip rip database

Description Display the RIP IPv4 route database.

Syntax

```
show ip rip database
```

Mode All

show ipv6 rip database

Description Display the RIP IPv4 route database.

Syntax

```
show ipv6 rip database
```

Mode All

RIP Clear Commands

This section lists the RIP clear commands.

clear ip rip route

Description Clears routes from the IPv4 RIP table.

Syntax

```
clear ip rip route {ipaddr/mask-length | rip}
```

Parameter	Description
ipaddr/mask-length	Clears 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 |
all |
bgp |
connected |
floating-ip |
ip-nat |
ip-nat-list |
isis |
ospf |
rip |
static |
vip [only-flagged | only-not-flagged]
}
```

Parameter	Description
ipv6addr/mask-length	Clears the route to the specified network.
all	Clears ***all*** RIP routes from the table.
bgp	Clears all RIP routes received from BGP.
connected	Clears all RIP routes to directly connected networks.
floating-ip	Clears all RIP routes to floating IP addresses.
ip-nat	Clears all RIP routes to translated NAT addresses allocated from a pool.
ip-nat-list	Clears all RIP routes to translated NAT addresses allocated from a range list.
isis	Clears all RIP routes received from IS-IS.
ospf	Clears all RIP routes received from OSPF.
static	Clears all static RIP routes.
vip [**only-flagged** | **only-not-flagged**]	Clears all RIP routes to virtual server IP addresses.

By default, routes to all VIPs are cleared. To clear routes to a subset of VIPs, use one of the following options:

`only-flagged` – Clears the RIP routes to only the VIPs on which the **redistribution-flagged** command is used.

`only-not-flagged` – Clears the RIP routes to all VIPs *except* those on which the **redistribution-flagged** command is used.

Note: The **kernel** option is not applicable.

Mode Privileged EXEC or any configuration level

Config Commands: Router – OSPF

This chapter describes the commands for configuring global OSPFv2 and OSPFv3 parameters.

Note: This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Enabling OSPF

To enable OSPF, use one of the following commands at the global configuration level of the CLI. Each command changes the CLI to the configuration level for the specified OSPFv2 process ID or OSPFv3 process tag.

Enabling OSPFv2

```
router ospf [process-id]
```

The *process-id* specifies the IPv4 OSPFv2 process to run on the AX device, and can be 1-65535.

Enabling OSPFv3

```
router ipv6 ospf [tag]
```

The *tag* specifies the IPv6 OSPFv3 process to run on the IPv6 link, and can be 1-65535.

Interface-level OSPF Commands

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. (See "Config Commands: Interface" on page 203.)

Show Commands

To display OSPF settings, use **show ip ospf** or **show ipv6 ospf** commands. (See "Show Commands" on page 689.)

Global Configuration Commands Applicable to OSPFv2 or OSPFv3

The following configuration commands are applicable to OSPFv2 and OSPFv3.

The commands in this section apply throughout the OSPFv2 process or OSPFv3 process in which the commands are entered.

area *area-id* default-cost

Description

Specify the cost of a default summary route sent into a stub area.

Syntax

```
[no] area area-id default-cost num
```

Parameter	Description
area-id	Area ID, either an IP address or a number.
num	Cost of the default summary route, 0-16777214.

Default

The default is 1.

Mode

OSPFv2 or OSPFv3

Example

The following command assigns a cost of 4400 to default summary routes injected into stub areas:

```
AX(config-router)#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-id	Beginning area ID.
range *area-id*	Ending area ID.
ipaddr	Subnet address for the range.
/mask-length	Network mask length for the range.
advertise	Generates Type 3 summary LSAs for the areas in the range.
not-advertise	Does not generate Type 3 summary LSAs. The networks are hidden from other networks.

Default

There is no default range configuration. When you configure a range, the default advertisement string is **advertise.**

Mode

OSPFv2 or OSPFv3

Example

The following command configures a range and disables advertisement of routes into the areas:

```
AX(config-router)#area 8.8.8.8 range 10.10.10.10/16 not-advertise
```

area *area-id* stub

Description

Configure a stub area.

Syntax

```
[no] area area-id stub [no-summary]
```

Parameter	Description
area-id	Area ID.
no-summary	ABRs do not send summary LSAs into the stub area.

Default

None

Mode

OSPFv2 or OSPFv3

Example

The following command configures a stub area with area ID 10.2.4.5:

```
AX(config-router)#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]
[hello-interval seconds]
[message-digest-key num md5 string [string ...]]
[retransmit-interval seconds]
[transmit-delay seconds]
```

Parameter	Description
area-id	Area ID, either an IP address or a number.
ipaddr	IP address of the OSPF neighbor at the other end of the link.
authentication	Enables authentication on the link.
authentication-key *string* [*string* ...]	Specifies a simple text password for authenticating OSPF traffic between this router and the neighbor at the other end of the virtual link. The *string* is an 8-character authentication password.
dead-interval *seconds*	Number of seconds this OSPF router will wait for a reply to a hello message sent to the neighbor on the other end of the virtual link, before declaring the neighbor to be offline. You can specify 1-65535 seconds.
hello-interval *seconds*	Number of seconds this OSPF router waits between sending hello messages to the neighbor on the other end of the virtual link. You can specify 1-65535 seconds.

message-digest-key *num* **md5** *string* [*string* ...]	Specifies an MD5 key, 1-255. The *string* is a 16-character authentication password.
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.
transmit-delay *seconds*	Number of seconds this OSPF router waits between sending packets to the neighbor on the other end of the virtual link. You can specify 1-65535 seconds.

Default

None. When you configure a virtual link, it has the following default settings:

- **authentication** – disabled
- **authentication-key** – not set
- **dead-interval** – 40
- **hello-interval** – 10
- **message-digest-key** – not set
- **retransmit-interval** – 5
- **transmit-delay** – 1

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
```

Parameter	Description
mbps	Specifies the reference bandwidth, in Mbps. You can specify 1-4294967.

Default

100 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

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`

Parameter	Description
num	Default cost, 0-16777214.

Default 20

Mode OSPFv2 or OSPFv3

Example The following command configures a default metric of 6666:

```
AX(config-router)#default-metric 6666
```

distribute-internal

Description

Enable redistribution of AX-specific resources as internal routes (type-1 LSAs).

Syntax

```
[no]  distribute-internal
{floating-ip | ip-nat | ip-nat-list | vip |
  vip-only-flagged}
area area-id
[cost num]
```

Parameter	Description
floating-ip [*options*]	Redistributes routes into OSPF for reaching HA 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.
area *area-id*	Specifies the OSPF area into which to redistribute the internal routes.
cost *num*	Specifies the cost for using the internally redistributed routes. You can specify 1-65535. The default is 1.

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 AX-specific resource type.

Example

The following command enables internal distribution into OSPF area 0, of routes to all VIPs configured on the AX device, and assigns cost 11 to the routes:

```
AX(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:

```
AX(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 HA floating IP addresses, and assigns cost 555 to the routes:

```
AX(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”.

```
AX(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 High Availability (HA).

Syntax

```
[no] ha-standby-extra-cost num
```

Parameter	Description
num	Specifies the extra cost to add to the AX device’s OSPF interfaces, if the HA status of one or more of the device’s HA groups 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 OSPF protocol on the AX device is not aware of the HA state (Active or Standby) of the AX device.

Mode OSPFv2 or OSPFv3

Usage Enter the command on each of the AX devices in the HA pair.

log-adjacency-changes

Description Log adjacency changes.

Syntax

```
[no] log-adjacency-changes [detail]
```

Default Disabled

Mode OSPFv2 or OSPFv3

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
```

Parameter	Description
num	Specifies 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.

maximum-area

Description Set the maximum number of OSPF areas supported for this OSPF process.

Syntax

```
[no] maximum-area num
```

Parameter	Description
num	Specifies the maximum number of areas allowed for this OSPF process. You can specify 1-4294967294.

Default 4294967294

Mode OSPFv2 or OSPFv3

passive-interface

Description Disable Link-State Advertisements (LSAs) from being sent on an interface.

Syntax

```
[no] passive-interface
{ethernet portnum | loopback num | management |
  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:

```
AX(config-router)#passive-interface ve 3
```

redistribute

Description

Enable distribution of routes from other sources into OSPF.

```
[no] redistribute
{
bgp [options] |
connected [options] |
floating-ip [options] |
ip-nat [ipaddr/mask-length
  floating-IP-forward-address ipaddr] [options] |
ip-nat-list [options] |
is-is [options] |
kernel [options] |
nat64 [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 BGP routes into OSPF. For *options*, see the end of this parameter list.
connected [*options*]	Redistributes routes into OSPF for reaching directly connected networks. For *options*, see the end of this parameter list.
floating-ip [*options*]	Redistributes routes into OSPF for reaching HA floating IP addresses. For *options*, see the end of this parameter list.
ip-nat [*ipaddr/mask-length* **floating-IP-forward-address** *ipaddr*] [*options*]	Redistributes routes into OSPF for reaching translated NAT addresses allocated from a pool. By default, the forward address for all redistributed NAT pool addresses is 0.0.0.0. To set a floating IP address as the forward address, use the *ipaddr/mask-length*] option to specify the

NAT pool address. The **floating-IP-forward-address** *ipaddr* option specifies the forward address to use when redistributing the route to the NAT pool address.

For *options*, see the end of this parameter list.

ip-nat-list [*options*]

Redistributes routes into OSPF for reaching translated NAT addresses allocated from a range list. For *options*, see the end of this parameter list.

is-is [*options*]

Redistributes IS-IS routes into OSPF. For *options*, see the end of this parameter list.

kernel [*options*]

The **kernel** options are not applicable to the current release and are not supported.

nat64 [*options*]

Redistributes routes into NAT64. For *options*, see the end of this parameter list. (This command applies to OSPFv3 and does not appear in the OSPFv2 CLI syntax.)

ospf [*process-id*] [*options*]

Redistributes routes into this OSPFv2 process for reaching networks in another OSPFv2 process. For *options*, see the end of this parameter list.

rip [*options*]

Redistributes RIP routes into OSPF.
For *options*, see the end of this parameter list.

static [*options*]

Redistributes routes into OSPF for reaching networks through static routes. For *options*, see the end of this parameter list.

vip [*ipaddr* **floating-IP-forward-address** *ipaddr* | {**only-flagged** | **only-not-flagged**}] [*options*]

Redistributes routes into OSPF for reaching virtual server IP addresses.

By default, the forward address for all redistributed VIPs is 0.0.0.0. To set a floating IP address as the forward address, use the *ipaddr* option to specify the VIP address. Use the **floating-IP-forward-address** *ipaddr* option to specify the forward address to use when redistributing the route to the VIP.

By default, all VIPs are redistributed when you use the **vip** option. To restrict redistribution to a subset of VIPs, use one of the following options:

> **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used.
>
> **only-not-flagged** – Redistributes all VIPs *except* those on which the **redistribution-flagged** command is used.
>
> For more information, see “Usage”.

For *options*, see below.

options

Optional parameters supported for all the options listed above:

metric-type {**1** | **2**} – External link type associated with the route advertised into the OSPF routing domain:

1 – Type 1 external route

2 – Type 2 external route

metric *num* – Metric for the route, 0-16777214. The default is 20.

route-map *map-name* – Name of a route map. (To configure a route map, see “route-map” on page 160.)

tag *num* – Includes the specified tag value in external Link-State Advertisements (LSAs).

Inter-domain routers running Border Gateway Protocol (BGP) can be configured to make routing decisions based on the tag value. The tag value can be 0-4294967295. The default is 0.

Note: The **kernel** options are not applicable to the current release and are not supported.

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. For example, if you use the **vip** option, routes to all VIPs are redistributed into OSPF.

By default, the AX 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 AX 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. They are mutually exclusive.

- 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 only-not-flagged** command is automatically converted into the **redistribute vip** command. When you display the configuration, it will contain the **redistribute vip** command, not the **redistribute vip only-not-flagged** command. This command conversion makes the behavior in the current release backwards compatible with the behavior in previous releases.

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**.)

Example The following commands redistribute floating IP addresses and VIP addresses into OSPF:

```
AX(config-router)#redistribute floating-ip
AX(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.

```
AX(config)#slb virtual-server vip1
AX(config-slb virtual server)#redistribution-flagged
AX(config-slb virtual server)#exit
AX(config)#router ospf
AX(config-router)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:

```
AX(config-router)#redistribute vip metric-type 1 metric 1 tag 555
```

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`

Default

For OSPFv2, the default router ID is the highest-numbered IP address configured on any of the AX device's loopback interfaces. If no loopback interfaces are configured, the highest-numbered IP address configured on any of the AX device's other Ethernet data interfaces is used.

For OSPFv3, the router ID must be set.

Note: Setting the router ID is required for OSPFv3 and is strongly recommended for OSPFv2.

Mode

OSPFv2 or OSPFv3

Usage

The AX device has only one router ID. The address does not need to match an address configured on the AX 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:

```
AX(config-router)#router-id 2.2.2.2
AX(config-router)#clear ip ospf process
```

timers spf exp

Description

Change Shortest Path First (SPF) timers used for route recalculation following a topology change. This command enables exponential back-off delays for route recalculation.

Syntax

```
[no] timers spf exp min-delay max-delay
```

Parameter	Description
min-delay	Specifies the minimum number of milliseconds (ms) the OSPF process waits after receiving a topology change, before recalculating its OSPF routes. You can specify 0-2147483647.
max-delay	Specifies the maximum number of milliseconds (ms) the OSPF process waits after receiving a topology change, before recalculating its OSPF routes. You can specify 0-2147483647.

Default

The default *min-delay* is 500 ms. The default *max-delay* is 50000 ms.

Mode

OSPFv2 or OSPFv3

Usage After you enter this command, any pending route recalculations are rescheduled based on the new timer values.

Global Configuration Commands Applicable to OSPFv2 Only

The following configuration commands are applicable to OSPFv2 only.

The commands in this section apply throughout the OSPFv2 process in which the commands are entered.

area *area-id* authentication

Description Enable authentication for an OSPF area.

Syntax

```
[no] area area-id authentication [message-digest]
```

Parameter	Description
message-digest	Enables MD5 authentication. If you omit this option, simple text authentication is used.

Default Disabled. No authentication is used.

Mode OSPFv2

Usage To configure a simple text password or MD5 key, see "ip ospf" on page 215.

area *area-id* filter-list

Description Filter the summary routes advertised by this OSPF router, if it is acting as an Area Border Router (ABR).

Syntax

```
[no] area area-id filter-list
{
access acl-id {in | out} |
prefix list-name {in | out}
}
```

Parameter	Description
`area-id`	Area ID, either an IP address or a number.
access *acl-id* {**in** | **out**}	ID of an Access Control List (ACL). The only routes that are advertised are routes to the subnets permitted by the ACL.
prefix *list-name* {**in** | **out**}	ID of an IP prefix list. The only routes that are advertised are routes to the subnets that match the list.

Default

Not set.

Mode

OSPFv2

Usage

You can specify an ACL ***or*** an IP prefix list. To configure an ACL, see “access-list (standard)” on page 80, “access-list (extended)” on page 82, or “ipv6 access-list” on page 266. To configure a prefix list, see “ip prefix-list” on page 254.

area *area-id* multi-area-adjacency

Description

Enables support for multiple OSPF area adjacencies on the specified interface.

Syntax

```
[no] area area-id multi-area-adjacency
{ethernet portnum | loopback num | management |
  ve ve-num}
neighbor ipaddr
```

Default

Disabled. By default, only one OSPF adjacency is allowed on an interface for a given OSPF process.

Mode

OSPFv2

Usage

This command is applicable only if this OSPF router is an ABR.

area *area-id* nssa

Description Configure a not-so-stubby area (NSSA).

Syntax

```
[no] area area-id nssa
[
default-information-originate
  [metric num] [metric-type {1 | 2}] |
no-redistribution |
no-summary |
translator-role {always | candidate | never}
]
```

Parameter	Description
area-id	Area ID.
default-information-originate [metric *num***] [metric-type {1 | 2}]**	Generates a Type 7 LSA into the NSSA area. (This option takes effect only on Area Border Routers (ABRs)). **metric** *num* – Metric for the default route, 0-16777214. The default is 20. **metric-type** {**1** | **2**} – External link type associated with the route advertised into the OSPF routing domain: **1** – Type 1 external route **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:

```
AX(config-router)#area 6.6.6.6 nssa
```

area *area-id* shortcut

Description Configure short-cutting through an area.

Syntax

```
[no] area area-id shortcut
{default | disable | enable}
```

Parameter	Description
area-id	Area ID.
default	Enables the default shortcut behavior. (See below.)
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.

capability opaque

Description Disable or re-enable opaque LSA capability.

Syntax

```
[no] capability opaque
```

Default Enabled.

Mode OSPFv2

Usage Opaque-LSAs deliver information used by external applications. Type 9, 10 and 11 LSAs can be opaque LSAs.

compatible rfc1583

Description Enable calculation of summary route costs per RFC 1583.

Syntax

```
[no] compatible rfc1583
```

Default Disabled. Summary route costs are calculated based on RFC 2328.

Mode OSPFv2

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 AX device to automatically declare itself a default gateway for other OSPF routers, even if the AX device does not have a default route to 0.0.0.0/0.
metric *num*	Metric for the default route, 0-16777214.
metric-type {**1** | **2**}	External link type associated with the default route advertised into the OSPF routing domain: **1** – Type 1 external route **2** – Type 2 external route
route-map *map-name*	Name of a route map. (To configure a route map, see “route-map” on page 160.)

Default This option is disabled by default. If you enable it, the default metric is 10. The default metric type is 2.

Mode

OSPF

Example

The following command creates a default route into the OSPF domain with a metric of 20:

```
AX(config-router)#default-information originate metric 20
```

distance

Description

Set the administrative distance for OSPF routes, based on route type.

Syntax

```
[no] distance
{
num |
ospf {external | inter-area | intra-area} num
}
```

Parameter	Description
num	Sets the administrative distance for all route types. You can specify 1-255.
ospf {external | inter-area | intra-area} *num*	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. You can use the **ospf** option with one or more of its suboptions. For each route type, you can specify 1-255.

Default

For all route types, the default administrative distance is 110.

Mode

OSPFv2

Usage

The administrative distance specifies the trustworthiness of routes. A low administrative distance value indicates a high level of trust. Likewise, a administrative distance value indicates a low level of trust. For example, setting the administrative distance value for external routes to 255 means those routes are very untrustworthy and should not be used.

distribute-list

Description

Filter the networks received or sent in route updates.

Syntax

```
[no] distribute-list acl-id
{
in |
out {connected | floating-ip | ip-nat |
  ip-nat-list | ospf | static | vip}
```

Parameter	Description
acl-id	ID of an ACL. Only the networks permitted by the ACL will be allowed.
in	Uses the specified ACL to filter routes received by OSPF from other sources. The filter applies to routes from all sources.
out *route-type*	Uses the specified ACL to filter routes advertised by OSPF to other routing domains. The *route-type* can be one of the following: **connected** – Filters advertisement of directly connected networks. **floating-ip** – Filters advertisement of networks for HA floating IP addresses. **ip-nat** – Filters advertisement of networks that are translated NAT addresses allocated from a pool. **ip-nat-list** – Filters advertisement of networks that are translated NAT addresses allocated from a range list. **ospf** [*process-id*] – Filters advertisement of networks to another OSPF process. **static** [**only-flagged** | **only-not-flagged**] – Filters advertisement of networks reached by static routes. **vip** [**only-flagged** | **only-not-flagged**] – Filters advertisement of networks to reach VIPs. By default, the option applies to all VIPs. To restrict the option to a subset of VIPs, use one of the following options:

only-flagged – Redistributes only the VIPs on which the **redistribution-flagged** command is used.

only-not-flagged – Redistributes all VIPs *except* those on which the **redistribution-flagged** command is used.

Note: The **bgp**, **isis**, and **kernel** options are not applicable to the current release and are not supported.

Default None

Mode OSPFv2

host *ipaddr* area

Description Configure a stub host entry for an area.

Syntax

```
[no] host ipaddr area area-id [cost num]
```

Parameter	Description
ipaddr	IP address of the host.
area *area-id*	OSPF area where the host is located.
cost *num*	Cost of the stub host entry, 0-65535.

Default None

Mode OSPFv2

Usage Routes to the host are listed in router LSAs as stub links.

neighbor

Description Configure an OSPF neighbor that is located on a non-broadcast network.

Syntax

```
[no] neighbor ipaddr
[
cost num |
poll-interval seconds [priority num] |
priority num [poll-interval seconds]
]
```

Parameter	Description
ipaddr	IP address of the OSPF neighbor.
cost *num*	Specifies the link-state metric to the neighbor, 1-65535.
poll-interval *seconds*	Number of seconds this OSPF router will wait for a reply to a hello message sent to the neighbor, before declaring the neighbor to be offline. You can specify 1-65535 seconds.
priority *num*	Router priority of the neighbor, 1-255.

Default

No neighbors on non-broadcast networks are configured by default. When you configure one, the other parameters have the following default settings:

- **cost** – not set
- **poll-interval** – 120 seconds
- **priority** – 0

Mode

OSPFv2

Usage

This command is required only for neighbors on networks. Adjacencies to neighbors on other types of networks are automatically established by the OSPF protocol.

It is recommended to set the poll-interval to a much higher value than the hello interval.

network

Description

Enable OSPF routing for an area, on interfaces that have IP addresses in the specified area subnet.

Syntax

```
[no] network
ipaddr {/mask-length | wildcard-mask}
area area-id
[instance-id num]
```

Parameter	Description
ipaddr {/mask-length | wildcard-mask}	Subnet of the area. You can specify the subnet in CIDR format (*ipaddr/mask-length*) or as *ipaddr wildcard-mask*. In a *wildcard-mask*, 0s represent

	the network portion and 1s represent the host portion. For example, for a subnet that has 254 hosts and a 24-bit network mask, the **wildcard-mask** is 0.0.0.255.
area *area-id*	Area ID.
instance-id *num*	Range of OSPF instances for which to enable OSPF routing for the area, 0-255. If you omit this option, OSPF routing is enabled for all OSPF instances that are running on interfaces that have IP addresses in the specified area subnet.

Default None

Mode OSPFv2

Example The following command configures an OSPF network:

```
AX(config-router)#network 10.10.20.20/24 area 10.10.20.30
```

ospf abr-type

Description Specify the Area Border Router (ABR) type.

Syntax

```
[no] ospf abr-type
{cisco | ibm | shortcut | standard}
```

Parameter	Description
cisco	Alternative ABR using Cisco implementation (RFC 3509).
ibm	Alternative ABR using IBM implementation (RFC 3509).
shortcut	Shortcut ABR (draft-ietf-ospf-shortcut-abr-02.txt).
standard	Standard ABR behavior (RFC 2328)

Default cisco

Mode OSPFv2

overflow database

Description

Specify the maxim number of LSAs or the maximum size of the external database.

Syntax

```
[no] overflow database
{
max-lsa [hard | soft] |
external max-lsa recover-time
}
```

Parameter	Description
max-lsa **[hard | soft]**	Specifies the maximum number of LSAs per OSPF process, 0-4294967294. The **hard** | **soft** option specifies the action to take if the LSA limit is exceeded: **hard** – Shut down the OSPF process for the process. **soft** – Issue a warning message without shutting down the OSPF process for the process.
external *max-lsa* *recover-time*	Specifies the maximum number of AS-external-LSAs the OSPF router can receive, 0-2147483647. The *recover-time* option specifies the number of seconds OSPF waits before attempting to recover after *max-lsa* is exceeded. You can specify 0-65535 seconds. To disable recovery, specify 0.

Default

The default *max-lsa* is 2147483647.

Mode

OSPFv2

summary-address

Description

Summarize or disable advertisement of external routes for a specific IP address range. A summary-address helps reduce the size of the OSPF link-state database.

Syntax

```
[no] summary-address ipaddr/mask
{not-advertise | tag num}
```

Parameter	Description
ipaddr/mask	Specifies the address range.
not-advertise	Disables advertisement of routes for the specified range.
tag *num*	Includes the specified tag value in external LSAs for IP addresses within the specified range. The tag value can be 0-4294967295. The default tag value is 0.

Default None

Mode OSPFv2

Global Configuration Commands Applicable to OSPFv3 Only

All the global OSPF commands that are applicable to OSPFv3 are also applicable to OSPFv2. (See "Global Configuration Commands Applicable to OSPFv2 or OSPFv3" on page 312.)

Interface-level Configuration Commands

The commands in this section apply only to the interface at whose configuration level you enter them.

ip ospf

Description Configure OSPFv2 parameters on a data interface.

Syntax

```
[no] ip ospf [ipaddr] parameter
```

Parameter	Description
ipaddr	Configures the parameter only for the specified IP address. Without this option, the parameter is configured for all IP addresses on the interface.
authentication [**message-digest** | **null**]	Type 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.

authentication-key *key-string*
Password used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. Applies to simple authentication only. Can be a string up to 8 characters long, with no blanks.

cost *number*
Numeric cost for using the interface, 1-65535.

database-filter all out
Blocks flooding of LSAs to the OSPF interface.

dead-interval *seconds*
Number of seconds that neighbor OSPF routers will wait for a new OSPF Hello packet from the AX Series before declaring this OSPF router (the AX Series) to be down, 1-65535 seconds.

disable all
Disables all OSPF packet processing on the interface.

hello-interval *seconds*
Number of seconds between transmission of OSPF Hello packets on this interface, 1-65535 seconds.

message-digest-key *key-id* **md5** *key-string*
Set of MD passwords used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. You can enter up to four key strings. Applies only to MD authentication. Key strings can be up to 16 characters long, with no blanks.

mtu
Specifies the Maximum Transmission Unit (MTU) for OSPF packets transmitted on the interface. You can specify 576-65535 bytes.

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.

network *network-type* — OSPF network type from the default for the media. You can specify one of the following:

broadcast – Broadcast network.

non-broadcast – Non-broadcast multiaccess (NBMA) network.

point-to-multipoint – Point-to-multipoint network.

point-to-point – Point-to-point network.

priority *number* — Eligibility of this OSPF router to be elected as the designated router (DR) or backup designated router (BDRs) for the routing domain, 0-255. 1 is the lowest priority and 255 is the highest priority.

resync-timeout *seconds* — Time to wait before resetting the adjacency with a neighbor, after receiving a restart signal from the neighbor. The resync-timeout is applicable if out-of-band resynchronization does not occur following the restart signal. You can specify 1-65535 seconds.

retransmit-interval *seconds* — Number of seconds between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface, 3-65535 seconds.

transmit-delay *seconds* — Number of seconds it takes to transmit Link State Update packets (route updates) on this interface, 1-65535 seconds. This amount is added to the ages of LSAs sent in the updates.

Default

The OSPF interface options have the following defaults:

- **authentication** – Not set
- **authentication-key** – Not set
- **cost** – 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** – Disabled. LSA flooding is permitted.
- **dead-interval** – 40 seconds
- **hello-interval** – 10 seconds

- **message-digest-key** – Not set
- **mtu** – The IP MTU set on the interface is used.
- **mtu-ignore** – 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** – depends on the media type
- **priority** – 1
- **resync-timeout** – 40 seconds
- **retransmit-interval** – 5 seconds
- **transmit-delay** – 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 AX Series does not participate in DR and BDR election.

For the **message-digest-key** *key-id* **md5** *key-string* option, the CLI lists the **encrypted** keyword. This keyword encrypts display of the string in the startup-config and running-config. Do not enter this keyword. The AX device automatically applies the keyword. Entering the keyword manually is not valid.

Example

The following command sets the OSPF priority on Ethernet interface 10 to 100:

```
AX(config-if:ethernet10)#ip ospf priority 100
```

ipv6 ospf cost

Description

Explicitly set the link-state metric (cost) for this OSPF interface.

Syntax

```
[no] ipv6 ospf cost num
```

Parameter	Description
num	Specifies 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
```

Parameter	Description
seconds	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
```

Parameter	Description
seconds	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]
```

Parameter	Description
num	Specifies an OSPFv3 process, 0-255. If you do not use this option, MTU checking on the interface is disabled for all OSPFv3 processes.

Default

MTU checking is enabled by default.

Mode

Interface

ipv6 ospf neighbor

Description

Configure an OSPFv3 neighbor that is located on a non-broadcast network reachable through this interface.

Syntax

```
[no] ipv6 ospf neighbor ipv6-addr
[
cost num [instance-id num] |
instance-id num |
poll-interval seconds [priority num]
  [instance-id num] |
priority num [poll-interval seconds]
  [instance-id num]
]
```

Parameter	Description
ipv6-addr	IPv6 address of the OSPF neighbor.
cost *num*	Specifies the link-state metric to the neighbor, 1-65535.
poll-interval *seconds*	Number of seconds this OSPFv3 interface will wait for a reply to a hello message sent to the neighbor, before declaring the neighbor to be offline. You can specify 1-65535 seconds.
priority *num*	Router priority of the neighbor, 1-255.

Default

No neighbors on non-broadcast networks are configured by default. When you configure one, the other parameters have the following default settings:

- **cost** – not set
- **poll-interval** – 120 seconds
- **priority** – 0

ipv6 ospf network

Description

Specify the network type.

Syntax

```
[no] ipv6 ospf network
{
broadcast |
non-broadcast |
point-to-multipoint |
point-to-point
}
[instance-id num]
```

Parameter	Description
broadcast	Broadcast network.
non-broadcast	Non-broadcast multiaccess (NBMA) network.
point-to-multipoint	Point-to-multipoint network.
point-to-point	Point-to-point network.
num	Specifies an OSPFv3 process, 0-255. If you do not use this option, MTU checking on the interface is disabled for all OSPFv3 processes.

Default

Depends on the media type.

Mode

Interface

ipv6 ospf priority

Description

Specify the 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
```

Parameter	Description
num	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
```

Parameter	Description
seconds	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
```

Parameter	Description
seconds	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

ospf

Description Configure OSPF on the interface.

Syntax

```
[no] ospf [ipaddr] parameter
```

Parameter	Description
authentication [message-digest | null]	Type 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.
authentication-key *key-string*	Password used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. Applies to simple authentication only. Can be a string up to 8 characters long, with no blanks.
cost *number*	Numeric cost for using the interface, 1-65535.
dead-interval *seconds*	Number of seconds that neighbor OSPF routers will wait for a new OSPF Hello packet from the AX Series before declaring this OSPF router (the AX Series) to be down, 1-65535 seconds.
hello-interval *seconds*	Number of seconds between transmission of OSPF Hello packets on this interface, 1-65535 seconds.
priority *number*	Eligibility of this OSPF router to be elected as the designated router (DR) or backup designated router (BDRs) for the routing domain, 0-255. 1 is the lowest priority and 255 is the highest priority.

`retransmit-interval` *`seconds`*	Number of seconds between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface, 3-65535 seconds.
`transmit-delay` *`seconds`*	Number of seconds it takes to transmit Link State Update packets (route updates) on this interface, 1-65535 seconds. This amount is added to the ages of LSAs sent in the updates.

Default

The OSPF interface options have the following defaults:

- **authentication** – Not set
- **authentication-key** – Not set
- **cost** – 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.
- **dead-interval** – 40 seconds
- **hello-interval** – 10 seconds
- **priority** – 1
- **retransmit-interval** – 5 seconds
- **transmit-delay** – 1 second

Mode

Interface

OSPF Show Commands

This section lists the OSPF show commands.

show {ip | ipv6} ospf

Description Display configuration information and statistics for OSPFv2 processes or OSPFv3 processes.

Syntax

```
show ip ospf [process-id]

show ipv6 ospf [tag]
```

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, settings for all configured OSPFv2 processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, settings for all configured OSPFv3 processes are displayed.

Mode Privileged EXEC and all configuration levels

Example The following command shows information for OSPFv2 process 0:

```
AX#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
 Supports Graceful Restart
 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 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:

```
AX#show ip ospf border-routers

OSPF process 0 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 3.3.3.3 [1] via 10.0.0.1, ve 1, ABR, ASBR, Area 0.0.0.1
```

show ip ospf database

Description Displays information about the OSPFv2 databases on the device.

Note: The options are different for OSPFv3. See “show ipv6 ospf database” on page 351.

Syntax

```
show ip ospf database
[
adv-router ipaddr |
{asbr-summary | external | network |
  nssa-external | opaque-area | opaque-as |
  opaque-link | router | summary}
    [[ipaddr [adv-router ipaddr]
    [self-originate]] | [adv-router ipaddr] |
    [self-originate]] |
max-age |
self-originate
]
```

Parameter	Description
adv-router *ipaddr*	Displays LSA information for the specified advertising router.
asbr-summary	Displays information about ASBR summary LSAs.
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:

ipaddr	Displays LSA information for a specific link-state ID (expressed as an IP address).
adv-router *ipaddr*	Displays LSA information for the specified advertising router.
self-originate	Displays information for LSAs originated by this OSPF router.

Mode Privileged EXEC and all configuration levels

Example

The following command shows the OSPFv2 database:

```
AX#show ip ospf database

                Router Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         1105 0x800000c9 0xcb72 2
2.2.2.2         2.2.2.2          638 0x80000008 0xdb92 2
3.3.3.3         3.3.3.3         1998 0x800000cb 0x47c1 2
4.4.4.4         4.4.4.4         1717 0x800000f6 0xe1d2 3

                Net Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum
10.0.0.1        3.3.3.3         1998 0x80000006 0xec1b
11.0.0.1        3.3.3.3          203 0x80000005 0x14ef
13.0.0.2        4.4.4.4         1717 0x80000006 0xbf3c
14.0.0.1        4.4.4.4         1962 0x80000004 0xf207

                Summary Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         3.3.3.3         1998 0x800000a3 0x99ed 0.0.0.0/0

                NSSA-external Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
1.0.100.1       1.1.1.1         1105 0x8000008e 0x942a E2 1.0.100.1/32    0
```

show ipv6 ospf database

Description

Displays information about the OSPFv3 databases on the device.

Syntax

```
show ipv6 ospf [tag] database
[
external |
grace |
inter-prefix |
inter-router |
intra-prefix |
link |
network |
router}
[adv-router ipaddr]
]
```

Parameter	Description
external	Displays information about external LSAs.
grace	Displays information about grace LSAs, used during graceful restart.
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.
links	Displays information about link LSAs.
network	Displays information about network LSAs.
router	Displays information about router LSAs.

Each option above supports the following suboption:

adv-router *ipaddr*	Displays LSA information for the specified advertising router.

Mode Privileged EXEC and all configuration levels

Example The following command shows the OSPFv3 database:

```
AX#show ipv6 ospf database

            OSPFv3 Router with ID (1.1.1.1) (Process *null*)

                Link-LSA (Interface ve 1)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.49        1.1.1.1         1121 0x8000008a 0xc927      1
0.0.0.8         3.3.3.3         1953 0x80000007 0x30cd      1

                Link-LSA (Interface ve 2)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.50        1.1.1.1         1121 0x80000096 0x08d8      1
0.0.0.8         4.4.4.4         1893 0x80000007 0xe638      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum    Link
0.0.0.0         1.1.1.1         1114 0x800000b1 0xcafa      2
0.0.0.0         2.2.2.2          904 0x800000ab 0x61a6      2
0.0.0.0         3.3.3.3         1953 0x80000094 0xe52a      2
0.0.0.0         4.4.4.4         1893 0x800000a8 0x846b      2
```

```
                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.8         3.3.3.3         1953 0x80000006 0xd40b
0.0.0.9         3.3.3.3          179 0x80000005 0xfedc
0.0.0.8         4.4.4.4         1893 0x80000006 0xd8fe
0.0.0.9         4.4.4.4          124 0x80000005 0x03d0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.32.0        3.3.3.3         1953 0x80000006 0x9cb3       1  Network-LSA
0.0.36.0        3.3.3.3          179 0x80000005 0x90ba       1  Network-LSA
0.0.32.0        4.4.4.4         1893 0x80000006 0xec58       1  Network-LSA
0.0.36.0        4.4.4.4          124 0x80000005 0xe05f       1  Network-LSA
```

show {ip | ipv6} ospf interface

Description Display OSPF information for an interface.

Syntax

```
show {ip | ipv6} ospf interface
{ethernet portnum | loopback num | management |
  trunk num | udld num | ve ve-num}
```

Mode Privileged EXEC and all configuration levels

Example The following command shows OSPFv2 information for interface VE 1:

```
AX#show ip ospf interface ve 1
ve 1 is up, line protocol is up
  Internet Address 10.0.0.2/24, Area 0.0.0.1 [NSSA], MTU 1500
  Process ID 0, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1
  Designated Router (ID) 3.3.3.3, Interface Address 10.0.0.1
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.0.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 1274173120
  Hello received 1218 sent 1158, DD received 3 sent 4
  LS-Req received 0 sent 1, LS-Upd received 52 sent 49
  LS-Ack received 27 sent 35, Discarded 0
```

show ip ospf multi-area-adjacencies

Description Display OSPFv2 multi-area adjacency information.

Syntax

```
show ip ospf multi-area-adjacencies
```

Mode Privileged EXEC and all configuration levels

Example The following command shows multi-area adjacency information:

```
AX#show ip ospf 1 multi-area-adjacencies
Multi-area-adjacency on interface eth1 to neighbor 20.20.20.10
Internet Address 20.20.20.11/24, Area 0.0.0.1, MTU 1500
Process ID 1, Router ID 10.10.10.10, Network Type POINTOPOINT, Cost: 10
Transmit Delay is 1 sec, State Point-To-Point
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 1229928206
Hello received 0 sent 513, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
```

show {ip | ipv6} ospf neighbor

Description Display information about OSPF neighbors.

Syntax

```
show ip ospf [process-id] neighbor
[ipaddr [detail]] |
[all] |
[detail [all]] |
[interface ipaddr]

show ipv6 ospf [tag] neighbor
[ipaddr [detail]] |
[detail [all]] |
[interface ipaddr]
```

Note: The **all** option applies only to OSPFv2.

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.

tag — Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes are displayed.

ipaddr [**detail**] — Displays information for the specified neighbor. For detailed information, use the **detail** option. For summary information, omit the **detail** option.

all — Includes neighbors whose status is Down. Without this option, down neighbors are not included in the output.

detail [**all**] — Displays detailed information for all neighbors. To include down neighbors in the output, use the **all** option.

interface *ipaddr* — Displays information for neighbors reachable through the specified IP interface.

Mode Privileged EXEC and all configuration levels

Example The following command shows information for OSPFv2 neighbors:

```
AX#show ip ospf neighbor

OSPF process 0:
Neighbor ID     Pri    State           Dead Time    Address         Interface Instance ID
3.3.3.3           1    Full/DR         00:00:31     10.0.0.1        ve 1       0
4.4.4.4           1    Full/DR         00:00:30     13.0.0.2        ve 2       0
```

show ip ospf redistributed

Description Display the routes that are being redistributed into OSPFv2.

Syntax

```
show ip ospf [process-id] redistributed
[
connected |
floating-ip |
ip-nat |
ip-nat-list |
isis |
kernel |
ospf [process-id] |
selected-vip
static |
vip
]
```

Note: The **bgp**, **isis**, and **kernel** options are not applicable to the current release and are not supported.

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPF processes is displayed.
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.
ospf [*process-id*]	Displays redistributed routes from other OSPFv2 processes.
selected-vip	Displays redistributed routes to SLB VIPs that are explicitly flagged for redistribution. This option is 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

Usage For more information on VIP redistribution, see “Usage” in “redistribute” on page 321.

show {ip | ipv6} ospf route

Description Display information for OSPFv2 routes.

Syntax

show ip ospf [*process-id*] **route**

show ipv6 ospf [*tag*] **route**

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes are displayed.

Mode Privileged EXEC and all configuration levels

Example The following command shows OSPFv2 routes:

```
AX#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
```

show ipv6 ospf topology

Description Display OSPFv3 topology information.

Syntax

show ipv6 ospf [*tag*] **topology**
[**area** *area-id*]

Parameter	Description
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes is displayed.
area *area-id*	Displays OSPFv3 topology information for the specified area.

Mode Privileged EXEC and all configuration levels

Example The following command shows the OSPFv3 topology:

```
AX#show ipv6 ospf topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
1.1.1.1            E   --
2.2.2.2                2          3.3.3.3              ve 1
                                  4.4.4.4              ve 2
3.3.3.3            E   1          3.3.3.3              ve 1
4.4.4.4            E   1          4.4.4.4              ve 2
```

show {ip | ipv6} ospf virtual-links

Description Display virtual link information.

Syntax

```
show ip ospf [process-id] virtual-links
```

```
show ipv6 ospf [tag] virtual-links
```

Parameter	Description
process-id	Specifies the OSPFv2 process. If you omit this option, information for all configured OSPFv2 processes are displayed.
tag	Specifies the OSPFv3 process. If you omit this option, information for all configured OSPFv3 processes are displayed.

Mode Privileged EXEC and all configuration levels

Example The following command shows information for OSPFv2 virtual links:

```
AX(config)#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
```

Config Commands: Router – IS-IS

This chapter describes the commands for configuring global Intermediate System to Intermediate System (IS-IS) parameters.

`Note:` This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Enabling IS-IS

Use the following command at the global configuration level to specify the IS-IS instance to configure.

```
router isis tag
```

The *tag* specifies the IS-IS instance to configure, and can be 1-65535.

This command changes the CLI to the configuration level for the specified IS-IS instance. At this level, use the following command to configure the Network Entity Title (NET):

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

Global IS-IS Configuration Commands

This section describes the global configuration commands for IS-IS.

address-family

Description

Configure this IS-IS instance to exchange IPv6 addresses with other IS-IS routers.

Syntax

```
[no] address-family ipv6 [unicast]
```

Parameter	Description
`unicast`	Enables unicast IPv6 addresses to be exchanged, in addition to multicast addresses. Without this option, only multicast addresses can be exchanged.

This command changes the CLI to the address-family configuration level, where the following commands are available.

(The other commands are common to all CLI configuration levels. See “Config Commands: Global” on page 79.)

Command	Description
`adjacency-check`	Enables IS-IS router adjacency based on Type-Length-Value (TLV) fields in IS-IS Hello packets between routers.
`default-information originate`	Enables advertisement of the default route in Link State Packets (LSPs) sent by this IS-IS instance.
`distance`	Sets the administrative distance, 1-255, for IS-IS routes.
`exit-address-family`	Exits from the address-family configuration level.

`[no] multi-topology [level-1 | level-1-2 | level-2] [transition]`
Enables multi-topology mode. The **transition** option accepts and generates both IS-IS IPv6 and multi-topology IPv6 TLVs.

`redistribute` *`option`*
Enables distribution of routes from other sources into IS-IS. For available options, see "redistribute" on page 373.

`summary-prefix` *`ipv6-addr/prefix`* `[level-1 | level-1-2 | level-2]`
Configures an IPv6 summary prefix.

Default Disabled. When you enable IPv6 exchange, the unicast option is disabled by default.

Mode IS-IS

Example The following command enables exchange of IPv6 multicast and unicast addresses with other IS-IS routers:

```
AX(config-router)#address-family ipv6 unicast
```

adjacency-check

Description Enable IS-IS router adjacency based on Type-Length-Value (TLV) fields in IS-IS Hello packets between routers.

Syntax `[no] adjacency-check`

Default Enabled.

Mode IS-IS

area-password

Description

Configure the password for authenticating IS-IS traffic between Level-1 routers.

Syntax

```
[no] area-password string
[authenticate snp {send-only | validate}]
```

Parameter	Description
string	Specifies the password.
authenticate snp {send-only | validate}	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

Usage

This command applies only to Level-1. To configure authentication for Level-2, see "domain-password" on page 365.

Example

The following command configures IS-IS to use password "isisl1pwd" to authenticate Level-1 IS-IS traffic within the area, including inbound and outbound SNP PDUs:

```
AX(config-router)#area-password isisl1pwd authenticate snp validate
```

authentication

Description

Configure 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.
`key-chain` *name* `[level-1	level-2]`	Specifies the name of the certificate key chain to use for authenticating IS-IS traffic. **level-1** – Applies only to Level-1 (intra-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.

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:

```
AX(config-router)#authentication send-only
AX(config-router)#authentication mode md5
AX(config-router)#key-chain chain1
AX(config-router)#no authentication send-only
```

bfd

Description Enable BFD on all interfaces for which IS-IS is running.

Syntax `[no] bfd all-interfaces`

Default Disabled

Mode IS-IS

default-information originate

Description Enable advertisement of the default route in Link State Packets (LSPs) sent by this IS-IS instance.

Syntax `[no] default-information originate`

Default Disabled

Mode IS-IS

Usage If the IPv4 or IPv6 data route tables contain a default route, the default route is included in Level-2 LSPs sent by this IS-IS instance. This command does not apply to Level-1 LSPs.

distance

Description Set the administrative distance for IS-IS routes.

Syntax

```
[no] distance num [system-id]
```

Parameter	Description
num	Specifies the distance, 1-255.
system-id	Assigns the distance only to routes from the router with the specified IS-IS system ID.

Default None

Mode IS-IS

Usage The administrative distance specifies the trustworthiness of routes. A low administrative distance value indicates a high level of trust. Likewise, a administrative distance value indicates a low level of trust. For example, setting the administrative distance value for external routes to 255 means those routes are very untrustworthy and should not be used.

domain-password

Description Configure the password for authenticating IS-IS traffic between Level-2 routers.

Syntax

```
[no] domain-password string
[authenticate snp {send-only | validate}]
```

Parameter	Description
string	Specifies the password.
authenticate snp {send-only | validate}	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

Usage This command applies only to Level-2. To configure authentication for Level-1, see “area-password” on page 362.

Example The following command configures IS-IS to use password “isisl2pwd” to authenticate Level-2 IS-IS traffic, including inbound and outbound SNP PDUs:

```
AX(config-router)#domain-password isisl2pwd authenticate snp validate
```

ha-standby-extra-cost

Description Enable IS-IS awareness of High Availability (HA).

Syntax

```
[no] ha-standby-extra-cost num
```

Parameter	Description
num	Specifies the extra cost to add to the AX device’s IS-IS interfaces, if the HA status of one or more of the device’s HA groups 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 AX device is not aware of the HA state (Active or Standby) of the AX device.

Mode IS-IS

Usage Enter the command on each of the AX devices in the HA pair.

hostname dynamic

Description Enable support for the Dynamic Hostname Exchange Mechanism (described RFC 2763) and System-ID-to-hostname translation.

Syntax

```
[no] hostname dynamic
```

Default Disabled

Mode IS-IS

ignore-lsp-errors

Description Disable checksum verification for inbound LSPs.

Syntax

```
[no] ignore-lsp-errors
```

Default Disabled. The checksums of inbound LSPs are verified.

Mode IS-IS

is-type

Description Specify the IS-IS routing level for this IS-IS instance.

Syntax

```
[no] is-type {level-1 | level-1-2 | level-2-only}
```

Parameter	Description
`level-1`	Level-1 (intra-area) only.
`level-1-2`	Level-1 and Level-2.
`level-2-only`	Level-2 (inter-area) only.

Default Level-1-2, unless another IS-IS instance on the AX device already is running at Level-2. In this case, the default is Level-1.

Mode IS-IS

Usage Only one IS-IS instance on the AX device can run Level-2 routing.

log-adjacency-changes

Description Log adjacency changes.

Syntax

```
[no] log-adjacency-changes [detail]
```

Default Disabled

Mode IS-IS

lsp-gen-interval

Description Configure the minimum interval for LSP regeneration.

Syntax

```
[no] lsp-gen-interval [level-1 | level-2] seconds
```

Parameter	Description
level-1 | level-2	Specifies the circuit type to which to apply the interval configuration.
seconds	Specifies the minimum number of seconds between each regeneration of the LSP. You can specify 1-120 seconds.

Default 30 seconds, for both Level-1 and Level2

Mode IS-IS

lsp-refresh-interval

Description Configure the LSP refresh interval.

Syntax

```
[no] lsp-refresh-interval seconds
```

Parameter	Description
seconds	Specifies the minimum number of seconds IS-IS must wait before refreshing an LSP. You can specify 1-65535 seconds.

Default 900

Mode IS-IS

Usage The lsp-refresh-interval must be smaller than the max-lsp-lifetime.

max-lsp-lifetime

Description Configure the LSP maximum lifetime.

Syntax

```
[no] max-lsp-lifetime seconds
```

Parameter	Description
seconds	Specifies the maximum number of seconds an LSP can remain in the database without being refreshed. You can specify 350-65535 seconds.

Default 1200

Mode IS-IS

Usage The max-lsp-lifetime must be larger than the lsp-refresh-interval.

metric-style

Description Configure the metric style to use for SPF calculation and for TLV encoding in LSPs.

Syntax

```
[no] metric-style
{
narrow
  [transition [level-1 | level-1-2 | level-2]] |
transition
  [level-1 | level-1-2 | level-2] |
wide
  [transition [level-1 | level-1-2 | level-2]]
}
```

Parameter	Description
narrow [transition [level-1 | level-1-2 | level-2]]	Supports 6-bit metric length for SPF calculation and TLV encoding. The **transition** option also allows 24-bit metrics for SPF calculation, but not for TLV encoding. **level-1** – Supports 24-bit SPF calculation only for circuit type Level-1. **level-2** – Supports 24-bit SPF calculation only for circuit type Level-2. **level-1-2** – Supports 24-bit SPF calculation for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)

transition [level-1 | level-1-2 | level-2]

Supports 6-bit and 24-bit metric lengths for SPF calculation and TLV encoding.

level-1 – Supports both metric lengths only for circuit type Level-1.

level-2 – Supports both metric lengths only for circuit type Level-2.

level-1-2 – Supports both metric lengths for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)

wide [transition [level-1 | level-1-2 | level-2]]

Supports 24-bit metric length for SPF calculation and TLV encoding.

The **transition** option also allows 6-bit metrics for SPF calculation, but not for TLV encoding.

level-1 – Supports 6-bit SPF calculation only for circuit type Level-1.

level-2 – Supports 6-bit SPF calculation only for circuit type Level-2.

level-1-2 – Supports 6-bit SPF calculation for circuit types Level-1 and Level-2. (This is the default, if the **transition** option is used.)

Default

Narrow, for Level-1 and Level-2 routing levels (**level-1-2**)

Mode

IS-IS

net

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

Syntax

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

Parameter	Description
area-address	Specifies the address of the IS-IS area.
system-id	Specifies the system ID.

Default None

Mode IS-IS

Usage Each IS-IS instance must have at least 1 NET.

The total length of the NET can be 8-20 bytes.

- The last (right-most) byte must be 00.
- The *system-id* must be 6 bytes long. For Level-1, the *system-id* must be unique within the area. For Level-2, the *system-id* must be unique within the entire domain.
- The *area-address* can be up to 13 bytes long.

You can configure more than 1 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 AX interfaces.

Syntax

```
[no] passive-interface
[
ethernet port-num |
loopback num |
management |
trunk num |
udld num |
ve ve-num
]
```

Parameter	Description
ethernet *port-num*	Disables routing updates from being sent on the specified Ethernet data port.
loopback *num*	Disables routing updates from being sent on the specified loopback interface.
management	Disables routing updates from being sent on the Ethernet management port.
trunk *num*	Disables routing updates from being sent on the specified trunk interface.
udld *num*	Disables routing updates from being sent on the specified Unidirectional Link Detection (UDLD) link.
ve *ve-num*	Disables routing updates from being sent on the specified Virtual Ethernet (VE) interface.

Note: The current release does not support the **loopback**, **trunk**, or **udld** option.

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.

```
[no] redistribute
{
connected [options] |
floating-ip [options] |
ip-nat [options] |
ip-nat-list [options] |
isis [options] |
nat64 [options] |
kernel [options] |
ospf [process-id] [options] |
static [options] |
vip [only-flagged | only-not-flagged] [options]
}
```

Parameter	Description
connected [*options*]	Redistributes routes into IS-IS for reaching directly connected networks. For *options*, see the end of this parameter list.
floating-ip [*options*]	Redistributes routes into IS-IS for reaching HA floating IP addresses. For *options*, see the end of this parameter list.
ip-nat [*options*]	Redistributes routes into IS-IS for reaching translated NAT addresses allocated from a pool. For *options*, see the end of this parameter list.

ip-nat-list [*options*]

Redistributes routes into IS-IS for reaching translated NAT addresses allocated from a range list. For *options*, see the end of this parameter list.

nat64 [*options*]

Redistributes OSPF routes into NAT64. For *options*, see the end of this parameter list.

ospf [*options*]

Redistributes OSPF routes into IS-IS. For *options*, see the end of this parameter list.

static [*options*]

Redistributes routes into IS-IS for reaching networks through static routes. For *options*, see the end of this parameter list.

vip [**only-flagged** | **only-not-flagged**] [*options*]

Redistributes routes into IS-IS for reaching virtual server IP addresses.

By default, all VIPs are redistributed when you use the **vip** option. To restrict redistribution to a subset of VIPs, use one of the following options:

> **only-flagged** – Redistributes only the VIPs on which the **redistribution-flagged** command is used.
>
> **only-not-flagged** – Redistributes all VIPs *except* those on which the **redistribution-flagged** command is used.
>
> For more information, see “Usage”.

For *options*, see below.

options

Optional parameters supported for all the options listed above:

level-1 – Redistributes only at the IS-IS area 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:

external – Uses the route's metric for comparison.

internal – 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. (To configure a route map, use the **route-map** command. See "route-map" on page 160.)

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. For example, if you use the **vip** option, routes to all VIPs are redistributed into IS-IS.

VIP Redistribution

VIP redistribution is not supported for VIPs on which destination NAT has been disabled. For example, VIP redistribution is not supported for VIPs that are configured for Direct Server Return (DSR).

You can exclude redistribution of individual VIPs using one or the other of the following methods. They are mutually exclusive.

- 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 only-not-flagged** command is automatically converted into the **redistribute vip** command. When you display the configuration, it will contain the **redistribute vip** command, not the **redistribute vip only-not-flagged** command. This command conversion makes the behavior in the current release backwards compatible with the behavior in previous releases.

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 command enables redistribution of IS-IS routes into OSPF:

```
AX(config-router)#redistribute ospf
```

Example

The following commands redistribute floating IP addresses and VIP addresses into IS-IS:

```
AX(config-router)#redistribute floating-ip
AX(config-router)#redistribute vip
```

Example

The following commands flag a VIP, then configure IS-IS to redistribute only that flagged VIP. The other (unflagged) VIPs will not be redistributed.

```
AX(config)#slb virtual-server vip1
AX(config-slb virtual server)#redistribution-flagged
AX(config-slb virtual server)#exit
AX(config)#router isis
AX(config-router)redistribute vip only-flagged
```

restart-timer

Description Configure the graceful-restart timer.

Note: The current release does not support graceful restart.

Syntax

```
[no] restart-timer seconds
[level-1 | level-1-2 | level-2]
```

Parameter	Description
seconds	Specifies the number of seconds IS-IS waits for LSP database synchronization. You can specify 5-65535 seconds.
level-1 | level-1-2 | level-2	Specifies the router level.

Default 60 seconds, for both Level-1 and Level-2.

Mode IS-IS

set-overload-bit

Description Disable use of this IS-IS router as a transit router during SPF calculation.

Syntax

```
[no] set-overload-bit
[on-startup {seconds | wait-for-bgp}]
[suppress {[external] [interlevel]}]
```

Parameter	Description
on-startup {*seconds* | **wait-for-bgp**}	Sets the overload bit only after startup of the IS-IS instance, and clears the bit based on one of the following options: *seconds* – Clears the overload bit after the specified number of seconds. You can specify 5-86400 seconds.

wait-for-bgp – Clears the overload bit after BGP signals that it has finished convergence.

– If BGP is not running, the overload bit is immediately cleared.

– If BGP is running but does not signal convergence within 10 minutes after the IS-IS instance starts, the overload bit is cleared.

Note: The current release does not support BGP.

`suppress {[external] [interlevel]}` Suppresses redistribution of specific types of reachability information during the overload state.

external – Suppresses redistribution of IP prefixes learned from other protocols. For example, redistribution of IP prefixes from OSPF is suppressed.

interlevel – Suppresses redistribution of IP prefixes learned from other IS-IS levels. For example, redistribution of IP prefixes from Level-2 to Level-1 is suppressed.

Default Disabled. The overload bit is not set, and this IS-IS router can be used as a transit (intermediate hop) router during SPF calculation.

Mode IS-IS

Usage IP prefixes that are directly connected to this IS-IS router continue to be reachable even when the overload bit is set.

spf-interval-exp

Description Configure the minimum and maximum delay between receiving a link-state or IS-IS configuration change, and SPF recalculation.

Syntax

```
[no] spf-interval-exp [level-1 | level-2]
min-delay max-delay
```

Parameter	Description
`level-1 | level-2`	Specifies the IS-IS level to which to apply the interval setting.

min-delay	Specifies the minimum number of milliseconds (ms) to wait before SPF recalculation following a link-state or IS-IS configuration change. You can specify 0-2147483647 ms.
max-delay	Specifies the maximum number of ms to wait. You can specify 0-2147483647 ms.

Default The default *min-delay* is 500 ms and the default *max-delay* is 50000 ms, for Level-1 and Level-2 routing levels.

Mode IS-IS

summary-address

Description Configure an IPv4 summary address to aggregate multiple IPv4 prefixes for advertisement.

Syntax

```
[no] summary-address ipaddr/mask-length
[level-1 | level-1-2 | level-2]
```

Parameter	Description
ipaddr/mask-length	Specifies the summary IPv4 address to advertise.
level-1 | level-1-2 | level-2	Specifies the IS-IS routing level to which to advertise the summary address. If you do not specify a routing level, the summary address is advertised at Level-2 only.

Default None

Mode IS-IS

Usage The summary address is advertised instead of the individual IP prefixes contained in the summary address. For example, if the IPv4 route table has routes to 192.168.1.x/24, 192.168.2.x/24, and 192.168.11.x/24, you can configure IS-IS to advertise summary address 192.168.0.0/16 instead of each of the individual prefixes.

Interface-level IS-IS Configuration Commands

In addition to global parameters, IS-IS has parameters on the individual interface level. To configure IS-IS on an interface, use the **interface** command to access the configuration level for the interface, then use the following commands.

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]`	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.
`key-chain` *name* `[level-1 | level-2]`	Specifies the name of the certificate key chain to use for authenticating IS-IS traffic.

level-1 – Applies only to Level-1 (intra-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.

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.

```
AX(config-if:ve3)#no isis authentication mode md5
```

isis bfd

Description

Disable BFD on an individual interface.

Syntax

```
[no] bfd disable
```

Default

Takes the value from the global BFD configuration.

Mode

Interface

isis circuit-type

Description Specify the IS-IS routing level (circuit type) for this interface.

Syntax

```
[no] circuit-type [level-1 | level-1-2 | level-2]
```

Parameter	Description
`level-1 | level-1-2 | level-2`	Specifies the IS-IS routing level.

Default level-1-2

Mode Interface

isis csnp-interval

Description Configure the interval between transmission of complete sequence number PDUs (CSNPs).

Syntax

```
[no] isis csnp-interval seconds
[level-1 | level-2]
```

Parameter	Description
seconds	Specifies the number of seconds to wait between transmission of CSNPs. You can specify 0-65535 seconds.
`level-1 | level-2`	Specifies the IS-IS routing level to which the interval setting applies.

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 padding

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 | minimal}
[level-1 | level-2]
```

Parameter	Description
seconds | **minimal**	Specifies the number of seconds between transmission of Hello packets to neighbors. You can specify 0-65535 seconds. For information about the **minimal** option, see "Usage" below.
level-1 | **level-2**	Specifies the IS-IS routing level to which the interval setting applies.

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
```

(For more information, see “isis hello-multiplier” on page 384.)

isis hello-multiplier

Description

Configure the multiplier used for calculating the neighbor hold time for Hello packets.

Syntax

```
[no] isis hello-multiplier num [level-1 | level-2]
```

Parameter	Description
num	Specifies the multiplier. You can specify 3-1000.
level-1 | level-2	Specifies the IS-IS routing level to which the multiplier setting applies.

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
```

Parameter	Description
ms	Specifies the minimum number of ms IS-IS will wait between transmission of LSPs. You can specify 1-4294967295 ms.

Default 33 ms

Mode Interface

Usage The LSP transmission interval helps avoid high CPU utilization on IS-IS neighbors during LSP floods, by allowing the neighbors time to send, receive, and process LSPs.

isis mesh-group

Description Configure mesh-group membership to control LSP flooding from this interface.

Syntax

```
[no] isis mesh-group {group-num | blocked}
```

Parameter	Description
group-num	Specifies the mesh group number. You can specify 1-4294967295. LSPs are flooded to all Level-1 or Level-2 IS-IS neighbors (as applicable), ***except*** to the neighbors who are in the same mesh group. LSPs are not flooded to the neighbors who are in the same mesh group as this interface.
blocked	Blocks flooding of LSPs on this interface.

Default None

Mode Interface

isis metric

Description Configure the default IS-IS metric (cost) for the interface.

Syntax

```
[no] isis metric num [level-1 | level-2]
```

Parameter	Description
num	Specifies the cost of using this interface as a link in an IS-IS route. You can specify 1-63.

level-1 | level-2	Specifies the IS-IS routing level to which the default metric setting applies.

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. (See "metric-style" on page 369.)

isis network

Description Configure the network type.

Syntax

```
[no] isis network {broadcast | point-to-point}
```

Parameter	Description
broadcast	The network is a broadcast network.
point-to-point	The network is a point-to-point network.

Default broadcast

Mode Interface

isis password

Description Configure the plain-text password for authentication of Hello packets sent and received on this interface.

Syntax

```
[no] isis password string [level-1 | level-2]
```

Parameter	Description
string	Specifies the password.
level-1 | level-2	Specifies the IS-IS routing level to which the password applies.

Default None

Mode Interface

Usage The password is applicable only if the authentication type is plain-text. (See “isis authentication” on page 380.)

isis priority

Description Configure this interface’s priority for Designated Integrated System (DIS) election.

Syntax

```
[no] isis priority num [level-1 | level-2]
```

Parameter	Description
num	Specifies the priority, 0-127.
level-1 | level-2	Specifies the IS-IS routing level to which the priority applies.

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 network type is broadcast. (See “isis network” on page 386.)

isis restart-hello-interval

Description Configure the amount of time this interface waits for acknowledgement from neighbors of its notification to restart IS-IS, before resending the notification.

Syntax

```
[no] isis restart-hello-interval seconds
[level-1 | level-2]
```

Parameter	Description
seconds	Specifies the number of seconds IS-IS waits to receive an acknowledgement of its restart notification. You can specify 1-65535 seconds.

Parameter	Description
level-1 | level-2	Specifies the IS-IS routing level to which the interval applies.

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 AX device inserts a Restart TLV in IS-IS Hello packets sent to neighbors on this interface. If the an acknowledgement of the restart notification si 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
```

Parameter	Description
seconds	Specifies the number of seconds IS-IS waits before resending an LSP that was dropped. You can specify 0-65535 seconds. 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" on page 386.)

isis wide-metric

Description Configure the length of a wide metric on the interface.

Syntax

```
[no] isis wide-metric num [level-1 | level-2]
```

Parameter	Description
num	Specifies the metric length. You can specify 1-16777214.
level-1 | level-2	Specifies the IS-IS routing level to which the metric applies.

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. (See “metric-style” on page 369.)

Show Commands for IS-IS

This section describes the show commands for IS-IS.

show ip isis [*tag*] route

Description Display the IPv4 IS-IS route table.

Syntax

```
show ip isis [tag] route
```

Parameter	Description
tag	Specifies 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:

```
AX(config)#show ip isis route

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    1.0.0.0/24          10          --               ethernet 11    --
L2   2.2.2.2/32          10          1.0.0.2          ethernet 11    0
```

show isis counter

Description Display IS-IS statistics.

Syntax **show isis counter**

Mode All

Example The following command shows IS-IS counters:

```
AX(config)#show isis counter
Area (null):
IS-IS Level-1 isisSystemCounterEntry:
  isisSysStatCorrLSPs: 0
  isisSysStatAuthTypeFails: 0
  isisSysStatAuthFails: 0
  isisSysStatLSPDbaseOloads: 0
  isisSysStatManAddrDropFromAreas: 1
  isisSysStatAttmptToExMaxSeqNums: 0
  isisSysStatSeqNumSkips: 0
  isisSysStatOwnLSPPurges: 0
  isisSysStatIDFieldLenMismatches: 0
  isisSysStatMaxAreaAddrMismatches: 0
  isisSysStatPartChanges: 0
  isisSysStatSPFRuns: 6

IS-IS Level-2 isisSystemCounterEntry:
  isisSysStatCorrLSPs: 0
  isisSysStatAuthTypeFails: 0
  isisSysStatAuthFails: 0
  isisSysStatLSPDbaseOloads: 0
  isisSysStatManAddrDropFromAreas: 1
  isisSysStatAttmptToExMaxSeqNums: 0
  isisSysStatSeqNumSkips: 0
  isisSysStatOwnLSPPurges: 0
  isisSysStatIDFieldLenMismatches: 0
  isisSysStatMaxAreaAddrMismatches: 0
  isisSysStatPartChanges: 0
  isisSysStatSPFRuns: 8
```

show isis [*tag*] database

Description Display the IS-IS database entries.

Syntax

```
show isis [tag] database
[lspid]
[detail]
[l1 | l2 | level-1 | level-2]
```

Parameter	Description
tag	Specifies the IS-IS tag (area). If you do not specify a tag value, database entries for all areas is displayed.
lspid	Specifies the ID of a specific LSP to display.
detail	Displays detailed contents of the LSPs. Without this option, summary information is displayed.
l1 | l2 | level-1 | level-2	Specifies the IS-IS routing level for which to display database entries.

Mode All

Example The following command shows the IS-IS database:

```
AX(config)#show isis database
Area (null):
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000003   0xB670        1002              0/0/0
0000.0000.0001.01-00* 0x00000001   0x21B9        1002              0/0/0
0000.0000.0002.00-00  0x00000007   0xD649        1013              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* 0x00000004   0xB471        1012              0/0/0
0000.0000.0001.01-00* 0x00000001   0x21B9        1002              0/0/0
0000.0000.0002.00-00  0x00000007   0x6401        1166              0/0/0
```

show isis interface

Description Display IS-IS information for interfaces.

Syntax

```
show isis interface
[
counter |
ethernet port-num |
loopback num |
management |
trunk num |
udld num |
ve ve-num
}
```

Parameter	Description
counter	Displays IS-IS interface status information and statistics.
ethernet *port-num*	Displays IS-IS information for the specified Ethernet data port.
loopback *num*	Displays IS-IS information for the specified loopback interface.
management	Displays IS-IS information for the specified loopback interface.
trunk *num*	Displays IS-IS information for the specified trunk interface.
udld *num*	Displays IS-IS information for the specified UDLD interface.
ve *ve-num*	Displays IS-IS information for the specified VE interface.

Mode All

Example The following command shows IS-IS interface information:

```
AX(config)#show isis interface
ethernet 11 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: 0x0000000D
    Local SNPA: 001f.a002.78ce
    IP interface address:
      1.0.0.1/24
    IPv6 interface address:
      3000::1/64
      fe80::21f:a0ff:fe02:78ce/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 1 seconds
    Next IS-IS LAN Level-2 Hello in 2 seconds
```

show isis [*tag*] topology

Description Display IPv4 IS-IS topology information.

Syntax **show isis topology** [**l1** | **l2** | **level-1** | **level-2**]

Parameter	Description
l1 | l2 | level-1 | level-2	Specifies the IS-IS routing level for which to display topology information.

Mode All

Example The following command shows IPv4 IS-IS topology information:

```
AX(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 11 001f.a001.a423

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 11 001f.a001.a42
```

show ipv6 isis [*tag*] route

Description Display the IPv6 IS-IS route table.

Syntax **show ipv6 isis** [*tag*] **route**

Parameter	Description
tag	Specifies 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:

```
AX(config)#show ipv6 isis route

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 11
L2   3222::/64 [10]
      via fe80::21f:a0ff:fe01:a423, ethernet 11
```

show ipv6 isis [*tag*] topology

Description Display IPv6 IS-IS topology information.

Syntax

```
show ipv6 isis [tag]
topology [l1 | l2 | level-1 | level-2]
```

Parameter	Description
tag	Specifies the IS-IS tag (area). If you do not specify a tag value, topology information for all areas is displayed.
l1 | **l2** | **level-1** | **level-2**	Specifies the IS-IS routing level for which to display topology information.

Mode All

Example The following command shows IPv6 IS-IS topology information:

```
AX(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 11 001f.a001.a423

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 11 001f.a001.a423
```

Config Commands: Router – BGP

This chapter describes the syntax for the Border Gateway Protocol (BGP) commands in AX Release 2.6.6. The commands are described in the following sections:

- “Enabling BGP” on page 395
- “BGP Configuration Commands” on page 396
- “BGP Show Commands” on page 432
- “BGP Clear Commands” on page 449

Note: This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Enabling BGP

To enable BGP on the AX device:

1. 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 AX device supports configuration of one local AS.

2. Specify the AX device's BGP router ID:

   ```
   bgp router-id ipaddr
   ```

3. Specify each of the AX 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: If you do not explicitly configure the AX device's BGP router ID, BGP sessions may become reset whenever there is an interface state change.

BGP Configuration Commands

The commands in this section apply globally to the BGP process running on the AX device.

Commands at the Global Configuration Level

The commands in this section are available at the global configuration level of the CLI.

bgp extended-asn-cap

Description Enable the AX device to send 4-octet BGP Autonomous System Number (ASN) capabilities.

Syntax

```
[no] bgp extended-asn-cap
```

Default Disabled; 2-octet ASN capabilities are enabled instead.

Mode Configuration mode

bgp nexthop-trigger

Description Configure BGP nexthop tracking.

Syntax

```
[no] bgp nexthop-trigger delay seconds

[no] bgp nexthop-trigger enable
```

Parameter	Description
`delay` *seconds*	Specifies the how long BGP waits before walking the full BGP table to determine which prefixes are affected by the nexthop changes, after receiving a trigger about nexthop changes. You can specify 1-100 seconds.
`enable`	Enables nexthop tracking.

Default BGP nexthop tracking is disabled by default. When you enable it, the default delay is 5 seconds.

Mode Configuration mode

Commands at the BGP Router Configuration Level

The commands in this section are available at the configuration level for the BGP routing process for an AS.

To access the BGP router configuration level, use the **router bgp** *AS-num* command at the global configuration level of the CLI.

address-family

Description Configure address family parameters.

Syntax

```
[no] address-family
{
ipv4 [multicast | unicast] |
ipv6 [unicast]
}
```

Parameter	Description
`ipv4 [multicast | unicast]`	Enters configuration mode for an IPv4 address family.
`ipv6 [unicast]`	Enters configuration mode for an IPv6 address family.

This command changes the CLI to the configuration level for the specified address family, where the following commands are available.

Command	Description
`[no] aggregate-address` *options*	See “aggregate-address” on page 400.
`[no] dampening` *options*	See “bgp dampening” on page 401.
`[no] distance`	See “distance” on page 405.
`exit-address-family`	Exits the address-family configuration level.
`[no] neighbor` *options*	See the following sections: – “neighbor activate” on page 407 – “neighbor as-origination-interval” on page 408 – “neighbor allowas-in” on page 408 – “neighbor capability” on page 409 – “neighbor collide-established” on page 410 – “neighbor connection-retry-time” on page 411 – “neighbor default-originate” on page 412 – “neighbor description” on page 412 – “neighbor disallow-infinite-holdtime” on page 413 – “neighbor distribute-list” on page 413 – “neighbor dont-capability-negotiate” on page 414 – “neighbor ebgp-multihop” on page 414 – “neighbor enforce-multihop” on page 415 – “neighbor fall-over” on page 415

		– “neighbor filter-list” on page 416 – “neighbor maximum-prefix” on page 417 – “neighbor next-hop-self” on page 417 – “neighbor override-capability” on page 418 – “neighbor passive” on page 418 – “neighbor password” on page 419 – “neighbor peer-group” on page 419 – “neighbor prefix-list” on page 420 – “neighbor remote-as” on page 421 – “neighbor remove-private-AS” on page 421 – “neighbor route-map” on page 422 – “neighbor send-community” on page 422 – “neighbor shutdown” on page 423 – “neighbor soft-reconfiguration” on page 424 – “neighbor strict-capability-match” on page 424 – “neighbor timers” on page 425 – “neighbor unsuppress-map” on page 425 – “neighbor update-source” on page 426 – “neighbor version” on page 427 – “neighbor weight” on page 427
	`[no] network` *`options`*	See “network” on page 428.
	`[no] redistribute` *`options`*	See “redistribute” on page 429.
Default	None	
Mode	BGP	

aggregate-address

Description

Configure an aggregate address.

Syntax

```
[no] aggregate-address ipaddr/mask-length
[as-set] [summary-only]
```

Parameter	Description
ipaddr/mask-length	IPv4 aggregate network address.

Note: If you are using the command at the address-family configuration level, the *ipv6addr* option is also supported.

as-set	Generates AS set path information.
summary-only	Filters more specific routes from updates.

Default

None

Mode

BGP

auto-summary

Description

Enable sending of summarized routes to BGP peers.

Syntax

```
[no] auto-summary
```

Default

Disabled

Mode

BGP

bgp bestpath always-compare-med

Description

Enable comparison of Multi-Exit Discriminator (MED) values for paths from BGP neighbors in different autonomous systems (ASs). When this option is enabled, if multiple paths that are otherwise equal have the same MED values, the path with the lowest MED value is preferred.

Syntax

```
[no] bgp always-compare-med
```

Default

Disabled

Mode

BGP

Usage

If you need to enable comparison of MEDs for multiple paths from BGP neighbors within the same AS, see “bgp deterministic-med” on page 403.

bgp bestpath

Description

Configure options to select the best of multiple paths for a route.

Syntax

```
[no] bgp bestpath
{as-path [ignore] | compare-routerid}
```

Parameter	Description
as-path [ignore]	Specifies whether to consider the AS path when selecting the best path for a route. – To consider the AS path, use the **as-path** option without the **ignore** option. – To ignore the AS path, use the **as-path ignore** option.
compare-routerid	Enables comparison of router IDs when comparing identical routes received from different neighbors. In this case, the route from the neighbor with the lowest route ID is selected.

Default

This command has the following default settings:

- **as-path** – AS-path consideration is enabled by default.
- **compare-routerid** – BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Mode

BGP

bgp dampening

Description

Configure the BGP response to route flapping, to minimize network disruption.

Syntax

```
[no] bgp dampening
{dampening-options | route-map  map-name}
```

Parameter	Description
dampening-options	Configures the dampening options: *reachability-half-life* – Specifies the reachability half-life, which is the time it takes the penalty to decrease to one-half of its current value. You can specify 1-45 minutes. *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. *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. *max-suppress-duration* – Specifies the maximum time that a dampened route is suppressed. You can specify 1-255 minutes.
route-map *map-name*	Applies the dampening settings only to routes that match the specified route map.

Default

This command has the following default values:

- *reachability-half-life* – 15 minutes
- *reuse-start* – 750
- *suppress-start* – 2000
- *max-suppress-duration* – 60 minutes (4 times the half-life time)
- **route-map** – none

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.
`local-preference` *num*	Specifies the local preference value for routes. You can specify 0-4294967295.

Default

This command has the following default values:

- **ipv4-unicast** – enabled
- **local-preference** – 100

Mode

BGP

bgp deterministic-med

Description

Enable comparison of Multi-Exit Discriminator (MED) values for multiple paths from BGP neighbors within the same autonomous system (AS).

Syntax

```
[no] bgp deterministic-med
```

Default

Disabled

Mode

BGP

Usage

If you need to enable comparison of MEDs for paths from BGP neighbors in different ASs, see “bgp bestpath always-compare-med” on page 400.

bgp enforce-first-as

Description

Deny any updates from BGP neighbors that do not contain the neighbor's AS at the beginning of the AS_PATH list in the update.

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 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 Sets the threshold for the number of route changes allowed before the AX device temporarily disables the BGP next-hop trigger.

Syntax

```
[no] bgp nexthop-trigger-count num
```

Parameter	Description
num	Specifies the maximum number of route changes allowed before the next-hop trigger is temporarily disabled. You can specify 0-127. If you specify 0, the nexthop trigger is not disabled regardless of the number of route changes.

Default 60

Mode BGP

bgp router-id

Description Configure the router ID.

Syntax

```
[no] bgp router-id ipaddr
```

Parameter	Description
ipaddr	IPv4 address.

Default If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If there are multiple loopback interfaces, the loopback interface with the highest numbered IP address is used.

If there are no loopback interfaces, the interface with the highest numbered IP address is used.

Mode BGP

bgp scan-time

Description Set the interval for BGP route next-hop scanning.

Syntax

```
[no] bgp scan-time seconds
```

Parameter	Description
seconds	Amount of time between scans. You can specify 0-60 seconds.

Default 60

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 AX device. The greater the distance, the lower the trust rating.

Syntax

```
[no] distance
{
admin-distance ipaddr/mask-length [acl-id] |
bgp external internal local
}
```

Parameter	Description
admin-distance ipaddr/mask-length [*acl-id*]	Overrides the configured administrative distance for specific prefixes. The **acl-id** option specifies an ACL that matches on the routes for which to override the default administrative distance. If you do not use this option, the distance is applied to all IPv4 BGP routes.
bgp *external internal local*	Administrative distance for different route types: *external* – Specifies the administrative distance for BGP routes learned from another AS. *internal* – Specifies the administrative distance for BGP routes learned from a neighbor within the same AS. *local* – Specifies the administrative distance for BGP routes redistributed from another route source on this AX device. For each route type, you can specify a distance value of 1-255.

Default

The following administrative distance values are used by default:

- *external* – 20
- *internal* – 200
- *local* – 200

Mode

BGP

neighbor activate

Description Enable the exchange of address family routes with a neighboring BGP router.

Syntax

```
[no] neighbor neighbor-id activate
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – 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 advertisement-interval

Description Configure the minimum interval between transmission of BGP route updates to a neighbor.

Syntax

```
[no] neighbor neighbor-id
advertisement-interval seconds
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
seconds	Minimum interval between route updates. You can specify 0-600 seconds.

Default The advertisement interval has the following default settings:

- eBGP – 30 seconds
- iBGP – 5 seconds

Mode BGP

neighbor allowas-in

Description Allow re-advertisement of all prefixes containing duplicate AS numbers.

Syntax

```
[no] neighbor neighbor-id allowas-in
[occurrences]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
occurrences	Maximum number of occurrences of a given AS number. You can specify 1-10.

Default Disabled

Mode BGP

neighbor as-origination-interval

Description Configure the interval between transmission of AS origination route updates.

Syntax

```
[no] neighbor neighbor-id
as-origination-interval seconds
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
seconds	Time between AS origination route updates. You can specify 1-600 seconds.

Default 15 seconds

Mode BGP

neighbor capability

Description Configure capability settings for the AX device’s BGP communication with a neighbor.

Syntax

```
[no] neighbor neighbor-id capability
{
dynamic |
orf prefix-list {both | receive | send} |
route-refresh
}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
dynamic	Enables the AX 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 AX device's ORF capability to the neighbor.

`both` – AX device can send ORF entries to the neighbor, as well as receive ORF entries from the neighbor.

`receive` – AX device can receive ORF entries from the neighbor, but can not send ORF entries to the neighbor.

`send` – AX device can send ORF entries to the neighbor, but can not receive ORF entries from the neighbor.

`route-refresh`

Enables advertisement of route-refresh capability to the neighbor. When this option is enabled, the AX 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 (AX 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 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
```

Parameter	Description
neighbor-id	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 graceful-restart.

Mode BGP

neighbor connection-retry-time

Description Configure the connection retry time for a neighbor.

Syntax

```
[no] neighbor neighbor-id connection-retry-time
seconds
```

Parameter	Description
neighbor-id	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.
seconds	Connection retry time. You can specify 1-65535 seconds.

Default 120 seconds

Mode BGP

neighbor default-originate

Description Enable transmission of a default route (0.0.0.0) to a neighbor.

Syntax

```
[no] neighbor neighbor-id default-originate
[route-map map-name]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
map-name	Route map that specifies the nexthop IP address.

Default Disabled

Mode BGP

neighbor description

Description Configure a description for a neighbor.

Syntax

```
[no] neighbor neighbor-id description string
[string ...]
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
string	String of up to 80 characters describing the neighbor.

Default None

Mode BGP

neighbor disallow-infinite-holdtime

Description

Disallow a neighbor to set the holdtime to “infinite” (0 seconds).

Syntax

```
[no] neighbor neighbor-id
disallow-infinite-holdtime
```

Parameter	Description
neighbor-id	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 distribute-list

Description

Filter route updates to or from a neighbor.

Syntax

```
[no] neighbor neighbor-id distribute-list
ip-access-list {in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
ip-access-list	ACL that matches on the routes to filter.
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 dont-capability-negotiate

Description Disable capability negotiation with a neighbor.

Syntax

```
[no] neighbor neighbor-id
dont-capability-negotiate
```

Parameter	Description
neighbor-id	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 ebgp-multihop

Description Enable the AX device to allow connections to eBGP peers on indirectly connected networks.

Syntax

```
[no] neighbor neighbor-id ebgp-multihop
```

Default Disabled

Mode BGP

Usage To prevent traffic loops, multihop is not established if the only route to the multihop peer is a default route.

neighbor enforce-multihop

Description

Enforce requirement of the neighbor to set up BGP peer sessions with the AX device over multiple router hops.

Syntax

```
[no] neighbor neighbor-id enforce-multihop
```

Default

Disabled

Mode

BGP

neighbor fall-over

Description

Enable fallover detection for a BGP neighbor using Bidirectional Forwarding Detection (BFD).

Syntax

```
[no] neighbor neighbor-id fall-over bfd
[
authentication key-id
  {md5 | meticulous-md5 | meticulous-sha1 | sha1 |
    simple} key-string [...] |
multihop
]
```

Parameter	Description
neighbor-id	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.
authentication *key-id type string*	Configures authentication for the BFD session with the BGP peer. The *key-id* can be 0-255. The *type* specifies the authentication type can can be one of the following: **md5** **meticulous-md5** **meticulous-sha1**

	sha1
	simple
	The *string* specifies the key string.
multihop	Enables support for neighbors that are multiple hops away from the AX device.

Default Not set

Mode BGP

neighbor filter-list

Description Filter route updates to or from a neighbor based on AS path.

Syntax

```
[no] neighbor neighbor-id filter-list
AS-path-access-list {in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
AS-path-access-list	AS path list. To configure an AS path list, use the following command at the global configuration level of the CLI: **ip as-path access-list**
in | out	Specifies the update direction to filter: **in** – Updates received from the neighbor are filtered. **out** – Updates sent to the neighbor are filtered before transmission.

Default None. By default, updates are not filtered.

Mode BGP

neighbor maximum-prefix

Description

Configure the maximum number of network prefixes that can be received in route updates from a neighbor.

Syntax

```
[no] neighbor neighbor-id maximum-prefix num
[threshold]
```

Parameter	Description
neighbor-id	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.
num	Maximum number of prefixes allowed. You can specify 1-1024.
threshold	Percentage of the allowed maximum at which a warning message is generated. You can specify 1-100.

Default

The default maximum is 128. The default threshold is 75 percent.

Mode

BGP

Usage

If the maximum is reached, the AX device brings down the BGP session with the peer.

neighbor next-hop-self

Description

Configure the AX device as the BGP next hop for a neighbor.

Syntax

```
[no] neighbor neighbor-id next-hop-self
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.

Default Disabled

Mode BGP

neighbor override-capability

Description Override the results of capability negotiation with a neighbor.

Syntax

```
[no] neighbor neighbor-id override-capability
```

Parameter	Description
neighbor-id	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

Mode BGP

neighbor passive

Description Do not initiate a TCP connection with the specified neighbor, but allow the neighbor to initiate a TCP connection with the AX device. Once the connection is up, BGP will work over the connection.

Syntax

```
[no] neighbor neighbor-id passive
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.

Default Disabled

Mode BGP

neighbor password

Description Enable MD5 encryption for BGP sessions with a BGP neighbor.

Syntax [**no**] **neighbor** *neighbor-id* **password** *string*

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address.
string	Password string, 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 can not begin with a blank space, and can not contain any of the following special characters: `' " < > & \ / ?`

Default Disabled

Mode BGP

Example The following command enables MD5 for the connection with eBGP neighbor 10.10.10.22:

```
AX(config)#router bgp 123
AX(config-router:device1)#neighbor 10.10.10.22 remote-as 456
AX(config-router:device1)#neighbor 10.10.10.22 password 1234567890abcde
```

neighbor peer-group

Description Add the AX device to a BGP peer group.

Syntax [**no**] **neighbor** *neighbor-id* **peer-group** *group-name*

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address.
group-name	Name of the peer group.

Default None

Mode BGP

neighbor prefix-list

Description Use a prefix list to filter route updates to or from a neighbor.

Syntax

```
[no] neighbor neighbor-id prefix-list list-name
{in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
list-name	Name of the prefix list.
in | out	Specifies the update direction to filter: **in** – Updates received from the neighbor are filtered. **out** – Updates sent to the neighbor are filtered before transmission.

Default By default, updates are not filtered.

Mode BGP

Usage Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The AX device begins the search at the top of the prefix list, with rule sequence number 1. Once a match or deny occurs, the AX 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 remote-as

Description

Configure an internal or external BGP (iBGP or eBGP) TCP session with another router.

Syntax

```
[no] neighbor neighbor-id remote-as AS-num
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
AS-num	Neighbor’s AS number.

Note: AS number 23456 is a reserved 2-octet AS number. An old BGP speaker (2-byte implementation) should be configured with 23456 as its remote AS number while peering with a non-mappable new BGP speaker (4-byte implementation).

Default

None

Mode

BGP

neighbor remove-private-AS

Description

Remove the private AS number from outbound updates.

Syntax

```
[no] neighbor neighbor-id remove-private-AS
```

Default

Disabled

Mode

BGP

neighbor route-map

Description

Apply a route map to incoming or outgoing routes.

Syntax

```
[no] neighbor neighbor-id route-map map-name
{in | out}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
map-name	Name of the route map.
in | out	Specifies the traffic direction to which to apply the route map: **in** – The route map is applied to routes received from the neighbor. **out** – The route map is applied to routes sent to the neighbor.

Default

None

Mode

BGP

neighbor send-community

Description

Send community attributes to a neighbor.

Syntax

```
[no] neighbor neighbor-id send-community
[both | extended | standard]
```

Parameter	Description
neighbor-id	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.

both	Sends both standard and extended community attributes.
extended	Sends only extended community attributes.
standard	Sends only standard community attributes.

Default By default, both standard and extended community attributes are sent to a neighbor. To explicitly send only the standard or extended community attribute, run the **bgp config-type** command with the standard parameter, before running this command.

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 AX device re-announces them to the neighbor.

Usage To prevent community attributes from being re-announced to the neighbor, use the "**no**" form of this command.

neighbor shutdown

Description Disable a neighbor.

Syntax

```
[no] neighbor neighbor-id shutdown
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – 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 soft-reconfiguration

Description

Configure the AX device to begin storing updates, without any consideration of the applied route policy.

Syntax

```
[no] neighbor neighbor-id soft-reconfiguration
inbound
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – 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 strict-capability-match

Description

Close the BGP connection to a neighbor if a capability value does not completely match the value on the AX device.

Syntax

```
[no] neighbor neighbor-id strict-capability-match
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.

Default

Enabled

Mode BGP

neighbor timers

Description Configure the timers for a neighbor.

Syntax

```
[no] neighbor neighbor-id timers
{interval holdtime | connect seconds}
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
interval holdtime	The *interval* specifies the amount of time between transmission of keepalive messages to the neighbor. You can specify 0-65535 seconds. The *holdtime* specifies the maximum amount of time the AX device will wait for a keepalive message from the neighbor before declaring the neighbor dead. You can specify 0-65535 seconds.
connect *seconds*	Connect timer. You can specify 0-65535 seconds. In ACTIVE state, the BGP router (AX device) will accept an incoming connection request from the peer before the connect time expires.

Default The default *interval* is 60 seconds. The default *holdtime* is 180 seconds. The default connect time is 0.

Mode BGP

neighbor unsuppress-map

Description Selectively leak more-specific routes to a neighbor.

Syntax

```
[no] neighbor neighbor-id unsuppress-map map-name
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
map-name	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 update-source

Description Allow internal BGP sessions to use any operational interface for TCP connections with a neighbor.

Syntax

```
[no] neighbor neighbor-id update-source interface
```

Parameter	Description
neighbor-id	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.
interface	Interface name or address.

Default IP address of the outgoing interface to the neighbor.

Mode BGP

neighbor version

Description Specify the BGP version supported by the AX device for BGP communication with a neighbor.

Syntax

```
[no] neighbor neighbor-id version 4
```

Parameter	Description
neighbor-id	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 4

Mode BGP

neighbor weight

Description Assign a weight value to routes learned from a neighbor.

Syntax

```
[no] neighbor neighbor-id weight num
```

Parameter	Description
neighbor-id	ID of the neighbor, which can be one of the following types of values: *ipv4ipaddr* – IPv4 address. *ipv6addr* – IPv6 address. *tag* – Name of a peer group.
num	Weight value assigned to routes learned from the neighbor. You can specify 0-65535.

Default 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.

network

Description

Specify the networks to be advertised by the AX device's BGP routing process.

Syntax

```
[no] network
{ipaddr/mask-length | ipaddr mask network-mask}
[route-map map-name]
```

Parameter	Description
ipaddr/mask-length | *ipaddr* **mask** *network-mask*	Network address and mask.
map-name	Route map used to set or modify a value.

Default

None

Mode

BGP

Usage

A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

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] |
nat64 [route-map map-name] |
ospf [route-map map-name] |
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.

`nat64 [route-map` ***`map-name`*****`]`**

Redistributes route information from NAT64 into BGP. The **route-map** option specifies the name of a configured route map.

`ospf [route-map` ***`map-name`*****`]`**

Redistributes route information from Open Shortest Path First (OSPF) into BGP. The **route-map** option specifies the name of a configured route map.

`static [route-map` ***`map-name`*****`]`**

Redistributes routes into BGP for reaching networks through static routes. The **route-map** option specifies the name of a configured route map.

`vip [only-flagged [route-map` ***`map-name`*****`] | only-not-flagged [route-map`** ***`map-name`*****`] | [route-map`** ***`map-name`*****`]]`**

Redistributes routes into BGP for reaching virtual server IP addresses.

By default, all VIPs are redistributed when you use the **vip** option. To restrict redistribution to a subset of VIPs, use one of the following options:

> **`only-flagged`** – Redistributes only the VIPs on which the **redistribution-flagged** command is used.
>
> **`only-not-flagged`** – Redistributes all VIPs *except* those on which the **redistribution-flagged** command is used.

For more information, see “Usage”.

The **route-map** option specifies the name of a configured route map.

Note: The **kernel** option is not applicable.

Default None

Mode BGP

synchronization

Description Enable IGP synchronization of routes learned through iBGP.

Syntax

```
[no] synchronization
```

Default Disabled

Mode BGP

timers

Description Configure the BGP keepalive and holdtime timer values.

Syntax

```
[no] timers bgp interval holdtime
```

Parameter	Description
interval	Specifies the amount of time between transmission of keepalive messages to neighbors. You can specify 0-65535 seconds.
holdtime	Specifies the maximum amount of time the AX 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

BGP Show Commands

This section lists the BGP show commands.

show [ip] bgp *ipv4addr*

Description

Display BGP network information for IPv4.

Syntax

```
show bgp
{
ipv4addr |
ipv4addr/mask-length [longer-prefixes]
}
```

Parameter	Description
ipv4addr | *ipv4addr/mask-length* [**longer-prefixes**]	IPv4 prefix and mask length. The **longer-prefixes** option includes prefixes that have a longer mask than the one specified.

Mode

All

show [ip] bgp *ipv6addr*

Description

Display BGP network information for IPv6.

Syntax

```
show bgp
{
ipv6addr |
ipv6addr/mask-length [longer-prefixes]
}
```

Parameter	Description
ipv6addr | *ipv6addr/mask-length*	IPv6 prefix and mask length. The **longer-prefixes** option includes prefixes that have a longer mask than the one specified.

Mode All

show bgp ipv4 {multicast | unicast}

Description Display BGP information for IPv4.

Syntax

```
show 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 |
inconsistent-as |
neighbors [ipv4addr | ipv6addr
  [advertised-routes | received prefix-filter |
   received-routes | routes]] |
prefix-list list-name |
quote-regexp string |
regexp string [string ...] |
route-map map-name |
summary
]
```

Parameter	Description
multicast | unicast	Specifies the IPv4 address family for which to display information.
ipv4addr | *ipv4addr/mask-length*	Network and mask information.
community [*community-number*] [*options*]	Displays routes matching the communities. Enter the community number in *AA***:***NN* format. The following options are supported: **exact-match** – Displays only communities that exactly match.

local-AS – Displays only communities that are not sent outside the local AS.

no-advertise – Displays only communities that are not sent advertised to neighbors.

no-export – Displays only communities that are not exported to the next AS.

community-list *list-name* [**exact-match**]

Displays routes matching the specified community list. The **exact-match** option displays only the routes that have exactly the same communities.

dampening {*options*}

Displays route-flap dampening information. You must specify one of the following options:

dampened-paths – Displays paths suppressed due to dampening.

flap-statistics – Displays flap statistics for routes.

parameters – Displays details for configured dampening parameters.

filter-list *list-name*

Displays routes that match the specified filter list.

inconsistent-as

Displays routes that have inconsistent AS Paths.

neighbors [*ipv4addr* | *ipv6addr* [*options*]]

Displays detailed information about TCP and BGP neighbor connections. The following options are supported:

advertised-routes – Displays the routes advertised to a BGP neighbor.

received prefix-filter – Displays all received routes, both accepted and rejected.

received-routes – Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first.

routes – Displays all accepted routes learned from neighbors.

prefix-list *list-name*	Displays routes that match the specified prefix list.
quote-regexp *string*	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).
regexp *string* [*string* ...]	Displays routes that match the specified AS-path regular expression(s).
route-map *map-name*	Displays routes that match the specified route map.
summary	Displays a summary of BGP neighbor status.

Mode All

show bgp ipv4 neighbors

Description Display information about IPv4 BGP neighbors.

Syntax

```
show bgp ipv4 neighbors
[ipv4addr | ipv6addr
  [advertised-routes |
   received prefix-filter |
   received-routes |
   routes]]
```

Parameter	Description
ipv4addr | *ipv6addr*	Network and mask information.
advertised-routes	Displays the routes advertised to a BGP neighbor.
received prefix-filter	Displays all received routes, both accepted and rejected.
received-routes	Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first.

routes	Displays all accepted routes learned from neighbors.

Mode All

show bgp ipv4 prefix-list

Description Display IPv4 routes that match the specified prefix list.

Syntax

```
show bgp ipv4 prefix-list list-name
```

Mode All

show bgp ipv4 quote-regexp

Description Display IPv4 routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).

Syntax

```
show bgp ipv4 quote-regexp string
```

Mode All

show bgp ipv4 summary

Description Display a summary of BGP IPv4 neighbor status.

Syntax

```
show bgp ipv4 summary
```

Mode All

show bgp ipv6

Description Display BGP information for IPv6.

Syntax

```
show bgp ipv6
[
ipv6addr |
ipv6addr/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 |
inconsistent-as |
multicast {ipv6addr |
  ipv6addr/mask-length [longer-prefixes]} |
neighbors [ipv4addr | ipv6addr
  [advertised-routes | received prefix-filter |
   received-routes | routes]] |
paths |
prefix-list list-name |
quote-regexp string |
regexp string [string ...] |
route-map map-name |
summary |
unicast {ipv6addr |
  ipv6addr/mask-length [longer-prefixes]} |
view view-name
]
```

Parameter	Description
ipv6addr | *ipv6addr/mask-length*	Network and mask information.
community [*community-number*] [*options*]	Displays routes for communities. Enter the community number in *AA*:*NN* format. The following options are supported: **exact-match** – Displays only communities that exactly match.

local-AS – Displays only communities that are not sent outside the local AS.

no-advertise – Displays only communities that are not sent advertised to neighbors.

no-export – Displays only communities that are not exported to the next AS.

community-list *list-name* [**exact-match**]

Displays routes matching the specified community list. The **exact-match** option displays only the routes that have exactly the same communities.

dampening {*options*}

Displays route-flap dampening information. You must specify one of the following options:

dampened-paths – Displays paths suppressed due to dampening.

flap-statistics – Displays flap statistics for routes.

parameters – Displays details for configured dampening parameters.

filter-list *list-name*

Displays routes that match the specified filter list.

inconsistent-as

Displays routes that have inconsistent AS Paths.

multicast {*ipv6addr* | *ipv6addr/mask-length* [**longer-prefixes**]}

Displays IPv6 routes for the specified multicast address family.

The **longer-prefixes** option includes prefixes that have a longer mask than the one specified.

neighbors [*ipv4addr* | *ipv6addr* [*options*]]

Displays detailed information about TCP and BGP neighbor connections. The following options are supported:

	advertised-routes – Displays the routes advertised to a BGP neighbor. **received prefix-filter** – Displays all received routes, both accepted and rejected. **received-routes** – Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first. **routes** – Displays all accepted routes learned from neighbors.
paths	Displays BGP path information.
prefix-list *list-name*	Displays routes that match the specified prefix list.
quote-regexp *string*	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).
regexp *string* [*string* ...]	Displays routes that match the specified AS-path regular expression(s).
route-map *map-name*	Displays routes that match the specified route map.
summary	Displays a summary of BGP neighbor status.
unicast {*ipv6addr* | *ipv6addr/mask-length* [**longer-prefixes**]}	Displays IPv6 routes for the specified unicast address family. The **longer-prefixes** option includes prefixes that have a longer mask than the one specified.
view *view-name*	Displays neighbors within the specified view.

Note: The **labeled** option is not applicable.

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 Display nexthop tree details.

Syntax

```
show bgp nexthop-tree-details
```

Mode All

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

Description Display routes for communities.

Syntax

```
show [ip] bgp community [community-number]
[exact-match] [local-AS] [no-advertise]
[no-export]
```

Parameter	Description
community-number	Community number, in *AA*:*NN* format.
exact-match	Displays only communities that exactly match.
local-AS	Displays only communities that are not sent outside the local AS.
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-info

Description Display all BGP community information.

Syntax

```
show ip bgp community-info
```

Mode All

show [ip] bgp community-list

Description Display routes for a specific community list.

Syntax

```
show [ip] bgp community-list list-name
[exact-match]
```

Parameter	Description
list-name	Displays routes matching the specified community list.
exact-match	Displays only the routes that have exactly the same communities.

Mode All

show [ip] bgp dampening

Description Display route-flap dampening information.

Syntax

```
show [ip] bgp dampening
{dampened-paths | flap-statistics | parameters}
```

Parameter	Description
dampened-paths	Displays paths suppressed due to dampening.
flap-statistics	Displays flap statistics for routes.
parameters	Displays details for configured dampening parameters.

Mode All

show [ip] bgp filter-list

Description Display routes that match a specific filter list.

Syntax

```
show [ip] bgp filter-list list-name
```

Mode All

show [ip] bgp inconsistent-as

Description Display routes that have inconsistent AS Paths.

Syntax

```
show [ip] bgp inconsistent-as
```

Mode All

show ip bgp ipv4

Description Display BGP information for IPv4.

Syntax

```
show ip bgp ipv4 {multicast | unicast}
[
ipv4addr |
ipv4addr/mask-length |
cidr-only |
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 |
inconsistent-as |
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
]
```

Parameter	Description
multicast | unicast	Specifies the IPv4 address family for which to display information.
cidr-only	Displays routes with non-natural network masks.
community [*community-number*] [*options*]	Displays routes matching the communities. Enter the community number in *AA*:*NN* format. The following options are supported: **exact-match** – Displays only communities that exactly match. **local-AS** – Displays only communities that are not sent outside the local AS.

	no-advertise – Displays only communities that are not sent advertised to neighbors. **no-export** – Displays only communities that are not exported to the next AS.
community-list *list-name* [**exact-match**]	Displays routes matching the specified community list. The **exact-match** option displays only the routes that have exactly the same communities.
dampening {*options*}	Displays route-flap dampening information. You must specify one of the following options: **dampened-paths** – Displays paths suppressed due to dampening. **flap-statistics** – Displays flap statistics for routes. **parameters** – Displays details for configured dampening parameters.
filter-list *list-name*	Displays routes that match the specified filter list.
inconsistent-as	Displays routes that have inconsistent AS Paths.
neighbors [*ipv4addr* | *ipv6addr* [*options*]]	Displays detailed information about TCP and BGP neighbor connections. The following options are supported: **advertised-routes** – Displays the routes advertised to a BGP neighbor. **received prefix-filter** – Displays all received routes, both accepted and rejected. **received-routes** – Displays the received routes from neighbor. To display all the received routes from the neighbor, configure BGP soft reconfiguration first. **routes** – Displays all accepted routes learned from neighbors.
paths	Displays BGP path information.

prefix-list *list-name*	Displays routes that match the specified prefix list.
quote-regexp *string*	Displays routes that match the specified AS-path regular expression. Enclose the regular expression string in double quotation marks (example: “regexp-string-1”).
regexp *string* [*string ...*]	Displays routes that match the specified AS-path regular expression(s).
route-map *map-name*	Displays routes that match the specified route map.
summary	Displays a summary of BGP neighbor status.

Mode All

show [ip] bgp neighbors

Description Display information about BGP neighbors.

Syntax

```
show [ip] bgp neighbors
[
ipv4addr | ipv6addr
  [
   advertised-routes |
   connection-retrytime |
   hold-time |
   keepalive |
   keepalive-interval |
   notification |
   open |
   rcvd-msgs |
   received prefix-filter |
   received-routes |
   routes |
   sent-msgs |
   update
  ]
]
```

Parameter	Description
ipv4addr | *ipv6addr*	Network and mask information.
advertised-routes	Displays the routes advertised to a BGP neighbor.
connection-retrytime	Displays the configured connection-retry-time value at the session establishment time with the neighbor.
hold-time	Displays the configured hold-time value of the neighbor at the session establishment time with the neighbor.
keepalive	Displays the number of keepalive messages sent to the neighbor throughout the session.
keepalive-interval	Displays the configured keepalive-interval value at the session establishment time with the neighbor.
notification	Displays the number of Notification messages sent to the neighbor throughout the session.
open	Displays the number of Open messages sent to the neighbor throughout the session.
rcvd-msgs	Displays the number of messages received from the neighbor throughout the session.
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.
sent-msgs	Displays the number of messages sent to the neighbor throughout the session.
update	Displays the number of Update messages sent to the neighbor throughout the session.

Mode All

show [ip] bgp paths

Description Display BGP path information.

Syntax

```
show [ip] bgp paths
```

Mode All

show [ip] bgp prefix-list

Description Display 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 scan

Description Display BGP scan status.

Syntax

```
show ip bgp scan
```

Mode All

show [ip] bgp summary

Description Display a summary of BGP neighbor status.

Syntax

```
show [ip] bgp summary
```

Mode All

show ip bgp view

Description Display neighbors of a specific view.

Syntax

```
show ip bgp view view-name
[
ipv4addr |
ipv4addr/mask-length |
ipv4 {multicast | unicast} summary |
neighbors [ipv4addr | ipv6addr] |
summary
]
```

Parameter	Description
view-name	Name of the view.
ipv4addr | *ipv4addr/mask-length*	Prefix and mask.
ipv4 {**multicast** | **unicast**} **summary**	Displays information for the specified IPv4 address family.
neighbors [*ipv4addr* | *ipv6addr*]	Displays information for the specified neighbor.

`summary`	Displays summary neighbor information.

Mode All

BGP Clear Commands

This section lists the BGP clear 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] |
ipv4 {multicast | unicast}
  {in [prefix-filter] | out | soft [in | out]} |
ipv6 unicast [soft] {in | out} |
out |
soft {in | out}
]
```

Parameter	Description
`in [prefix-filter]`	Clears incoming advertised routes. The **prefix-filters** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration.
**`ipv4 {multicast	unicast}`** *`{options}`*	Clears routes for the specified IPv4 address family. You must specify one of the following options: **`in [prefix-filter]`** – Clears incoming advertised routes. The **prefix-filters** option pushes out prefix-list outbound routing filters, and performs inbound soft reconfiguration. **`out`** – Clears outgoing advertised routes. **`soft [in	out]`** – Clears the specified routes without resetting the BGP neighbor connection.

`in` – Requests route updates from the specified neighbor.

`out` – Sends route updates to the specified neighbor.

`ipv6 unicast [soft] {in | out}` – Clears routes for the IPv6 address family.

`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.

Note: The **ipv4** and **ipv6** options apply only to the **clear ip bgp** command, not the **clear bgp** command.

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] |
ipv4 {multicast | unicast}
  {in [prefix-filter] | out | soft [in | out]} |
out |
soft {in | out}
]
```

For option information, see “clear [ip] bgp {* | AS-num}” on page 449.

Note: The **ipv4** option applies only to the **clear ip bgp** command, not the **clear bgp** command.

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}
]
```

For option information, see "clear [ip] bgp {* | AS-num}" on page 449.

Note: The **ipv4** option applies only to the **clear ip bgp** command, not the **clear bgp** command.

Mode Privileged EXEC and all configuration levels

clear ip bgp dampening

Description Reset all dampened BGP routes.

Syntax

```
clear ip bgp dampening
[ipv4addr | ipv4addr/mask-length]
```

Parameter	Description
ipv4addr | ipv4addr/mask-length	Resets dampened routes only for the specified IPv4 prefix.

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}
]
```

For option information, see “clear [ip] bgp {* | AS-num}” on page 449.

Note: The **ipv4** option applies only to the **clear ip bgp** command, not the **clear bgp** command.

Mode Privileged EXEC and all configuration levels

clear ip bgp flap-statistics

Description Reset route-flap statistics counters and history.

Syntax

```
clear ip bgp flap-statistics
[ipv4addr | ipv4addr/mask-length]
```

Parameter	Description
ipv4addr | ipv4addr/mask-length	Resets route-flap statistics only for the specified IPv4 prefix.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp ipv4

Description Reset dampened routes or route-flap statistics counters and history for IPv4.

Syntax

```
clear [ip] bgp ipv4 {multicast | unicast}
{dampening | flap-statistics}
[ipv4addr | ipv4addr/mask-length]
```

Parameter	Description
dampening	Resets dampened routes.
flap-statistics	Resets route-flap statistics and history.
ipv4addr | ipv4addr/mask-length	Resets dampened routes or route-flap statistics and history only for the specified IPv4 prefix.

Mode Privileged EXEC and all configuration levels

clear [ip] bgp ipv6

Description Reset dampened routes or route-flap statistics counters and history for IPv6.

Syntax

```
clear [ip] bgp ipv6 unicast
{dampening | flap-statistics}
[ipv6addr | ipv6addr/mask-length]
```

Parameter	Description
dampening	Resets dampened routes.
flap-statistics	Resets route-flap statistics and history.
ipv6addr | ipv6addr/mask-length	Resets dampened routes or route-flap statistics and history only for the specified IPv6 prefix.

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] |
ipv4 {multicast | unicast}
  {in [prefix-filter] | out | soft [in | out]} |
out |
soft {in | out}
]
```

For option information, see "clear [ip] bgp {* | AS-num}" on page 449.

Note: The **ipv4** option applies only to the **clear ip bgp** command, not the **clear bgp** command.

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 *
[
in [prefix-filter] |
ipv4 {multicast | unicast}
  {in [prefix-filter] | soft {in | out}} |
soft {in | out}
]
```

For option information, see “clear [ip] bgp {* | AS-num}” on page 449.

Note: The **in** and **ipv4** options apply only to the **clear ip bgp** command, not the **clear bgp** command.

Mode

Privileged EXEC and all configuration levels

Config Commands: Large Scale NAT

The commands in this chapter configure Large Scale NAT (LSN).

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See "backup system" on page 50 and "backup log" on page 48.
- **clear** – See "clear" on page 59.
- **debug** – See "debug" on page 64.
- **do** – See "do" on page 117.
- **end** – See "end" on page 123.
- **exit** – See "exit" on page 124.
- **no** – See "no" on page 155.
- **show** – See "Show Commands" on page 689.
- **write** – See "write terminal" on page 78.

LSN Configuration Commands

This section describes the LSN configuration commands.

class-list (for LSN)

Description Configure an IP class list for use with Large Scale NAT (LSN).

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a file.

This command changes the CLI to the configuration level for the specified class list, where the following command is available.

Note: The other configuration commands at this level are not applicable to LSN.

Command	Description
`[`**`no`**`]` *`priv-addr`* `{`*`subnet-mask`*` | `*`/mask-length`*`}` `{`**`glid`**` `*`num`*` |` **`lid`**` `*`num`*` |` **`lsn-lid`**` `*`num`*`}`	Specifies the internal clients. The *priv-addr* option specifies the internal host or subnet address. Use the *subnet-mask* or */mask-length* option to specify the subnet mask or mask length. The **glid** *num* option specifies an global LSN LID to apply to matching clients. (See “glid” on page 125.) The **lid** *num* option specifies a non-LSN LID to apply to matching clients. The **lsn-lid** *num* option specifies an LSN LID to apply to matching clients. (See “lsn-rule-list” on page 482.)

Default

None

Mode

Configuration mode

Usage

Configure the LSN LIDs or Fixed-NAT LIDs before configuring the class list entries.

As an alternative to configuring class entries on the AX device, you can configure the class list using a text editor on another device, then import the class list onto the AX device. To import a class list, see “import” on page 69.

For more information about LSN, see the “Large Scale NAT” chapter in the *AX Series 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:

```
AX(config)#class-list list1
AX(config-class list)#5.5.5.0 /24 lsn-lid 5
```

ip nat inside (for LSN)

Description Bind an IP class list for use with LSN.

Syntax

```
[no] ip nat inside source class-list list-name
```

Parameter	Description
class-list *list-name*	Specifies 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 AX device. For more information, see the “Large Scale NAT” chapter in the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.

ip nat lsn alg

Description Disable or re-enable Application Level Gateway (ALG) support for LSN.

Syntax

```
[no] ip nat lsn alg
{esp | ftp | pptp | rtsp | sip | tftp}
{enable | disable}
```

Parameter	Description
esp	Enables or disables NAT64 ALG support for Encapsulating Security Payload (ESP).
ftp	Enables or disables NAT64 ALG support for File Transfer Protocol (FTP).
pptp	Enables or disables NAT64 ALG support for Point-to-Point Tunneling Protocol (PPTP).
rtsp	Enables or disables NAT64 ALG support for Real Time Streaming Protocol (RTSP).
sip	Enables or disables NAT64 ALG support for Session Initiation Protocol (SIP).
tftp	Enables or disables NAT64 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

ip nat lsn alg sip rtp-stun-timeout

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

Syntax

```
[no] ip nat lsn alg sip rtp-stun-timeout minutes
```

Parameter	Description
minutes	Specifies the timeout. You can specify 2-10 minutes.

Default 5

Mode Configuration mode

Usage The command applies to SIP ALG sessions for LSN, NAT64, and DS-Lite.

ip nat 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] ip nat 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.

ip nat lsn endpoint-independent-filtering

Description

Configure endpoint-independent filtering.

Syntax

```
[no] ip nat lsn endpoint-independent-filtering
[tcp | udp]
{
default |
disable {ephemeral | well-known |
  port-num [to port-num]} |
enable {ephemeral | well-known |
  port-num [to port-num]}
}
```

Parameter	Description
`tcp | udp`	Specifies the Layer 4 protocol. If you omit this option, the command applies to both TCP and UDP.
`default`	Uses the default behavior. (See “Default” below.)
`disable`	Disables endpoint-independent filtering. Use one of the following options to specify the ports: `ephemeral` – Disables endpoint-independent filtering for ports 1024-65535. `well-known` – Disables endpoint-independent filtering for well-known ports (1-1023). *port-num* [to *port-num*] – Disables endpoint-independent filtering for the specified port or port range.
`enable`	Enables endpoint-independent filtering. Use one of the following options to specify the ports: `ephemeral` – Enables endpoint-independent filtering for ports 1024-65535. `well-known` – Enables endpoint-independent filtering for well-known ports (1-1023).

port-num [to *port-num*] – Enables endpoint-independent filtering for the specified port or port range.

Default

Disabled for ports 1-1023. Enabled for ports 1024-65535.

Mode

Configuration mode

Usage

The following combinations of endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF) are not supported for the same destination port or port range:

- For a given destination port or range, EIF enabled with EIM disabled is not supported. For example, the following configuration for ports 2000-3000 is invalid:

  ip nat lsn endpoint-independent-mapping disable 2000 to 3000
  ip nat lsn endpoint-independent-filtering enable ephemeral

- For a given destination port or range, EIM enabled with EIF disabled is not supported.

ip nat lsn endpoint-independent-mapping

Description

Configure endpoint-independent mapping.

Syntax

```
[no] ip nat lsn endpoint-independent-mapping
[tcp | udp]
{
default |
disable {ephemeral | well-known |
  port-num [to port-num]} |
enable {ephemeral | well-known |
  port-num [to port-num]}
}
```

Parameter	Description
tcp | udp	Specifies the Layer 4 protocol. If you omit this option, the command applies to both TCP and UDP.
default	Uses the default behavior. (See "Default" below.)
disable	Disables endpoint-independent mapping. Use one of the following options to specify the ports: **ephemeral** – Disables endpoint-independent mapping for ports 1024-65535. **well-known** – Disables endpoint-independent mapping for well-known ports (1-1023). *port-num* [**to** *port-num*] – Disables endpoint-independent mapping for the specified port or port range.
enable	Enables endpoint-independent mapping. Use one of the following options to specify the ports:

ephemeral – Enables endpoint-independent mapping for ports 1024-65535.

well-known – Enables endpoint-independent mapping for well-known ports (1-1023).

port-num [**to** *port-num*] – Enables endpoint-independent mapping for the specified port or port range.

Default

Disabled for ports 1-1023. Enabled for ports 1024-65535.

Mode

Configuration mode

Usage

The following combinations of endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF) are not supported for the same destination port or port range:

- For a given destination port or range, EIF enabled with EIM disabled is not supported. For example, the following configuration for ports 2000-3000 is invalid:

  ip nat lsn endpoint-independent-mapping disable 2000 to 3000
  ip nat lsn endpoint-independent-filtering enable ephemeral

- For a port or range, EIM enabled with EIF disabled is not supported.

ip nat lsn full-cone

Description

Configure full-cone support.

Note: Enabling or disabling full-cone support is like enabling or disabling both endpoint-independent filtering ***and*** endpoint-independent mapping.

Syntax

```
[no] ip nat lsn full-cone disable
{
default |
disable {ephemeral | well-known |
  port-num [to port-num]} |
enable {ephemeral | well-known |
  port-num [to port-num]}
}
```

Parameter	Description
default	Uses the default behavior. (See “Default” below.)
disable	Disables full-cone support. Use one of the following options to specify the ports:

Parameter	Description
	ephemeral – Disables full-cone support for ports 1024-65535. **well-known** – Disables full-cone support for well-known ports (1-1023). *port-num* [**to** *port-num*] – Disables full-cone support for the specified port or port range.
enable	Enables full-cone support. Use one of the following options to specify the ports: **ephemeral** – Enables full-cone support for ports 1024-65535. **well-known** – Enables full-cone support for well-known ports (1-1023). *port-num* [**to** *port-num*] – Enables full-cone support for the specified port or port range.

Default Disabled for ports 1-1023. Enabled for ports 1024-65535.

Mode Configuration mode

ip nat lsn hairpinning

Description Configure filtering for hairpinning.

Syntax

```
[no] ip nat lsn hairpinning
{filter-self-ip | filter-self-ip-port}
```

Parameter	Description
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-self-ip-port**

Mode Configuration mode

ip nat lsn icmp

Description

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

Syntax

```
[no] ip nat lsn icmp
{send-on-port-unavailable |
send-on-user-quota-exceeded}
{
admin-filtered |
disable |
enable |
host-unreachable
}
```

Parameter	Description
send-on-port-unavailable	Sends ICMP Destination Unreachable message when there are no protocol ports available for NAT mappings.
send-on-user-quota-exceeded	Sends ICMP Destination Unreachable message when a a user quota is exceeded.
admin-filtered	Sends code type 3, code 13, administratively filtered.
disable	Disable ICMP Unreachable messages for the specified event.
enable	Enables ICMP Unreachable messages for the specified event. (This option is not applicable to **send-on-user-quota-exceeded**.)
host-unreachable	Sends code type 3, code 1 for IPv4, and type 1 code 3 for IPv6.

Default

The default for **send-on-port-unavailable** is **disable**. The default for **send-on-user-quota-exceeded** is **admin-filtered**.

Mode

Configuration mode

ip nat lsn ip-selection

Description Specify the method for LSN to use to select IP addresses within a pool.

Syntax

```
[no] ip nat lsn ip-selection method
```

Parameter	Description
method	Specifies the method, which can be 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.

ip nat lsn logging default-template

Description

Set a configured LSN traffic logging template as the default template for all LSN pools.

Syntax

```
[no] ip nat lsn logging default-template
template-name
```

Parameter	Description
template-name	Specifies 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. To configure a NAT logging template, see "ip nat template logging" on page 479.

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. See "ip nat lsn logging pool" on page 466.

Example

The following commands configure a NAT logging template, then set it as the default logging template for LSN:

```
AX5200(config)#slb server syslog1 192.168.1.100
AX5200(config-real server)#port 514 udp
AX5200(config-real server)#exit
AX5200(config)#slb service-group syslog udp
AX5200(config-slb svc group)#member syslog1:514
AX5200(config-slb svc group)#exit
AX5200(config)#ip nat template logging lsn_logging
AX5200(config-nat logging)#log port-mappings
AX5200(config-nat logging)#service-group syslog
AX5200(config-nat logging)#exit
AX5200(config)#ip nat lsn logging default-template lsn_logging
```

ip nat lsn logging pool

Description Assign a NAT logging template to an LSN pool.

Syntax

```
[no] ip nat lsn logging pool pool-name template
template-name
```

Parameter	Description
pool-name	Specifies the LSN pool.
template-name	Specifies the NAT logging template.

Default Not set. If a NAT logging template has been set as the default NAT logging template, that template is used.

Mode Configuration mode

Usage The NAT logging template you plan to use must already be configured. To configure a NAT logging template, see “ip nat template logging” on page 479.

ip nat 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] ip nat lsn port-batching size
{1 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024}
```

Parameter	Description
1 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024	Specifies the number of ports to allocate in each batch.

Default Disabled

Mode Configuration mode

ip nat lsn port-overloading allow-different-user

Description Allows an overloaded port to be used by more than one client.

Syntax

```
[no] ip nat 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

ip nat lsn port-overloading enable

Description Enable Port Overloading.

Syntax

```
[no] ip nat lsn port-overloading enable
[
ephemeral |
well-known |
{tcp | udp} port-num [to port-num]}
]
```

Parameter	Description
`ephemeral`	Enables port overloading for ports 1024-65535.
`well-known`	Enables port overloading for well-known ports, 1-1023.

`{tcp	udp}`
	`port-num`
	`[to` *`port-num`*`]`
		Enables port overloading for the specified protocol and port or port range.

Default Port overloading is enabled for all ports, 1-65535.

Mode Configuration mode

ip nat lsn port-overloading unique

Description

Change the granularity for Port Overloading.

Syntax

```
[no] ip nat 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

ip nat lsn port-reservation

Description

Configure static LSN mappings for a range of protocol ports for an internal address.

Syntax

```
[no] ip nat lsn port-reservation inside
priv-ipaddr start-priv-portnum end-priv-portnum
nat public-ipaddr start-public-portnum
end-public-portnum
```

Parameter	Description
priv-ipaddr	Specifies the internal IP address.
start-priv-portnum	Specifies the beginning (lowest-numbered) protocol port number in the range of internal protocol port numbers.
end-priv-portnum	Specifies the ending (highest-numbered) protocol port number in the range of internal protocol port numbers.

public-ipaddr	Specifies the public IP address to map to the internal IP address.
start-public-portnum	Specifies the beginning public protocol port number in the range to map to the internal protocol port numbers.
end-public-portnum	Specifies the ending public protocol port number in the range to map to the internal protocol port numbers.

Default

None. If LSN is configured, LSN mappings are created and deleted dynamically.

Mode

Configuration mode

ip nat lsn radius server

Description

Create a RADIUS server configuration. This option can be useful for logging client attributes, such as mobile numbers, obtained from an external RADIUS server.

Syntax

```
[no] ip nat lsn 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. See “Config Commands: Global” on page 79.)

Parameter	Description
[no] attribute {inside-ip | inside-ipv6 | msisdn | imei | imsi} [[vendor *vendor-id*] **number** *attr-id*]	Specifies the RADIUS attributes for the AX device to receive from external RADIUS servers in response to RADIUS Accounting requests. The following attributes can be specified:

`inside-ip` – Inside client's IPv4 address.

`inside-ipv6` – Inside client's IPv6 address.

`msisdn` – Inside client's mobile number, as Mobile Station International ISDN Number (MSISDN).

`imei` – Inside client's mobile number, as International Mobile Equipment Identity (IMEI).

`imsi` – Inside client's mobile number, as International Mobile Subscriber Identity (IMSI).

The *vendor-id* specifies the RADIUS vendor ID and can be 1-65535. The *attr-id* specifies the RADIUS attribute ID and can be 1-255. These options, in combination, allow you to specify any attribute to be used as the client's inside IP address, or MSIDSN, or IMEI, and so on. For example, if your RADIUS server normally sends the MSIDSN attribute as attribute 31, you could use the following command to configure the AX device to use the same attribute value for MSIDSN: **attribute msisdn number 31**

`[no]` **`listen-port`** *`portnum`*

Specifies the port number on which the external RADIUS server listen for Accounting requests. The default is 1813.

`[no]` **`remote ip-list`** *`list-name`*

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.

`[no]` **`secret`** *`shared-secret`*

Specifies the password string the external RADIUS servers and AX device use to authenticate RADIUS traffic between them.

Default

By default, no RADIUS servers are configured. When you use this command to configure one, the server has the following defaults:

- **attribute** – not set
- **listen-port** – 1813

- **remote ip-list** – not set
- **secret** – not set

Introduced in Release 2.6.6-P4

Mode Configuration mode

ip nat 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] ip nat lsn stun-timeout
[tcp | udp]
{ephemeral | well-known |
  port port-num [to port-num]}
minutes
```

Parameter	Description
`tcp | udp`	Specifies the Layer 4 protocol. If you omit this option, the command applies to both TCP and UDP.
`ephemeral`	Applies the command only to ports 1024-65535.
`well-known`	Applies the command only to ports 1-1023.

`port` *`port-num`*
`[to` *`port-num`*`]`
	Specifies an individual port or a custom port range.

`minutes`	Specifies the timeout, 0-60 minutes.

Default 2, for all TCP and UDP ports (1-65535)

Mode Configuration mode

Usage If you do not use the **ephemeral**, **well-known**, or **port** option, the command applies to ports 1-65535.

The AX device supports separate TCP and UDP configuration values for the LSN STUN timeout. Beginning in AX Release 2.6.6-P4, if the LSN STUN timeout has the same value for both TCP and UDP, the configuration appears as a single command in the running-config and configuration file.

Example in 2.6.6-P4 and Later:

```
ip nat lsn stun-timeout 1
```

Example of Same Configuration in Previous Releases:

```
ip nat lsn stun-timeout tcp 1
ip nat lsn stun-timeout udp 1
```

ip nat lsn syn-timeout

Description Configure the SYN timeout for LSN.

Default `[no] ip nat lsn syn-timeout seconds`

Parameter	Description
seconds	Specifies the timeout, 2-7 seconds.

Default 4

Mode Configuration mode

Usage The LSN SYN timeout is separate from the IP NAT translation timeout. If you need to configure the IP NAT translation timeout out instead, see "ip nat translation" on page 253.

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

Parameter	Description
none	Does not change the MSS value.
fixed *n*	Changes the MSS to the length you specify.
subtract *s* [**min** *n*]	Reduces the MSS if it is longer than the specified number of bytes. This option sets the MSS based on the following calculations:

– If MSS minus *S* is greater than *N*, subtract *S* from the MSS.

– If MSS minus *S* is less than or equal to *N*, set the MSS to *N*.

The subtract method of MSS clamping is used by default, with the following values:

S = 40 bytes

N = 416 bytes

Using these values, the default MSS clamping calculations are as follows:

– If MSS minus 40 is greater than 416, subtract 40 from the MSS.

– If MSS minus 40 is less than or equal to 416, set the MSS to 416.

Default

The **subtract** option is used by default. See above.

Mode

Configuration mode

ip nat lsn tcp reset-on-error

Description

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

Syntax

```
[no] ip nat lsn tcp reset-on-error outbound
{enable | disable}
```

Default

Enabled

Mode

Configuration mode

ip nat pool (for LSN)

Description

Configure a named set of IP addresses for use by Large Scale NAT (LSN).

Syntax

```
[no] ip nat pool pool-name
start-ipaddr end-ipaddr
netmask {subnet-mask | /mask-length}
lsn [max-users-per-ip num]
[gateway ipaddr]
[ha-group-id group-id [ha-use-all-ports]]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | /*mask-length*}	Network mask for the IP addresses in the pool.
lsn [**max-users-per-ip** *num*]	Enables the pool to be used for Large Scale NAT (LSN). The **max-user-per-ip** option specifies the maximum number of internal addresses that can be mapped to a single public address at the same time. You can specify 1-65535. By default, there is no limit.

Note: The **lsn** option applies only to the LSN feature. Pools that use the **lsn** option can not be used with any type of NAT except LSN.

Parameter	Description
gateway *ipaddr*	Default gateway to use for NATted traffic.
ha-group-id *group-id* [**ha-use-all-ports**]	HA group ID, 1-31. The **ha-use-all-ports** option disables division of the pool's ports between AX devices. Without this option, the AX device automatically allocates half of each pool address's ports to one of the AX devices and allocates the other half of the ports to the other AX device. (See "Usage" below.)

Note: It is recommended to use the **ha-use-all-ports** option only for DNS virtual ports. Using this option with other virtual port types is not valid.

Default None.

Mode Configuration mode

Usage The pool can be used by other **ip nat** commands. The IP addresses must be IPv4 addresses. To configure a pool of IPv6 addresses, see "ipv6 nat pool" on page 270.

To enable inside or outside NAT on interfaces, see “ip nat” on page 214.

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.

For conditions under which the NAT gateway is needed, if no NAT gateway is configured, the AX device uses the default gateway configured for the AX device’s other traffic instead.

Port Allocation Between AX Devices in High Availability Deployments (ha-use-all-ports option)

By default, when you assign an IP NAT pool to an HA group, the AX device automatically allocates half of each pool address’s ports to one of the AX devices and allocates the other half of the ports to the other AX device.

This automatic allocation is used to prevent simultaneous use of the same port number by both AX devices. For example, without this protection, it would be possible for the same IP address and protocol port number to be in use on both AX devices in an Active-Active configuration.

However, this protection also requires the pool to be configured with more addresses than will actually be needed.

In some cases, there is no benefit to dividing the pool’s ports between the AX devices. In particular, there is no benefit for DNS virtual ports. DNS sessions are very short-lived and are never synchronized between the AX devices. For this reason, there is no risk that the same NAT port will be in use on more than one session at the same time. You can use the **ha-use-all-ports** option to disable division of the ports between AX devices.

Note: It is recommended to use the **ha-use-all-ports** option only for DNS virtual ports. Using this option with other virtual port types is not valid.

Example

The following command configures an IP address pool named “pool1” that contains addresses from 30.30.30.1 to 30.30.30.254:

```
AX(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
[ha-group-id group-id]
```

Parameter	Description
pool-group-name	Name of the pool group.
ha-group-id *group-id*	HA group ID, 1-31.

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. See “Config Commands: Global” on page 79.)

Parameter	Description
member *pool-name*	Name of a configured IP address pool.

Default

None.

Mode

Configuration mode

Usage

To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

For Large Scale NAT (LSN), a pool group can contain up to 25 pools. For other types of NAT, a pool group can contain up to 5 pools. Pool group members must belong to the same protocol family (IPv4 or IPv6) and must use the same HA ID. A pool can be a member of multiple pool groups.

If a pool group contains pools in different subnets, the AX 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 AX selects the pool that is in the subnet for the outbound route.

The AX 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:

```
AX(config)#ip nat pool-group group1
AX(config-pool-group)member pool1
AX(config-pool-group)member pool2
AX(config-pool-group)member pool3
...
AX(config-pool-group)member pool25
```

ip nat template http-alg

Description

Configure a template for HTTP Application Level Gateway (ALG).

Syntax

[no] ip nat template http-alg *template-name*

Parameter	Description
template-name	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. See “Config Commands: Global” on page 79.)

Command	Description
[**no**] **request-insert-client-ip** [*options*]	Enables insertion of the client IP address into the headers of client HTTP requests. You can specify the following *options*: **header-name** *string* – Header name to insert, instead of the default. **include-tunnel-ip** – Includes the tunnel IP Address in the inserted header. This option applies only to DS-Lite sessions and 6rd-NAT64 sessions. **method** {**append** | **replace**} **header-name** *string* – 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-name is “X-Client-IP,” it will be replaced by the new “X-Client-IP” in the HTTP request.

If the packet has more than one header field of the same name, all of them will be replaced.

[**no**] **request-insert-msisdn** [**header-name** *string*] **radius-sg** *group-name* **secret** *string*

Inserts the client’s mobile number in client requests.

header-name *string* – Header name to insert, instead of the default.

radius-sg *group-name* **secret** *string* – Specifies the group of external RADIUS accounting servers to use for obtaining client mobile numbers.

group-name – Name of the service group that contains the client RADIUS servers.

string – Authentication string the AX device and the client RADIUS servers use to authenticate RADIUS traffic from one another.

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

Introduced in Release 2.6.6-P4

ip nat template logging

Description Configure a template for external logging of LSN traffic events. (See "Config Commands: Logging Template" on page 593.)

lsn-lid

Description Configure a limit ID (LID) for LSN.

Note: Some LSN LID commands apply only to other features, and are described in the chapters for those features.

Syntax

```
[no] lsn-lid num
```

Parameter	Description
num	LSN LID number, 1-31.

This command changes the CLI to the configuration level for the specified LSN LID, where the following commands are available.

Note: The other configuration commands at this level are not applicable to LSN.

Command	Description
[no] **drop-on-nat-pool-mismatch**	Drops traffic from users if their current NAT pool does not match that of the LSN LID. Disabled by default.
[no] **ds-lite inside-src-permit-list** *list-name*	For Dual-stack Lite (DS-Lite), uses a class list to specify the hosts or subnets that are permitted to

be NATted. Any IPv4 addresses that do not match the class list are not NATted.

[no] extended-user-quota {tcp | udp} service-port *portnum* **sessions** *num*

Configures a per-user extended quota for essential services. The **port** option specifies the Layer 4 protocol port of the service, and can be 1-65535. The **sessions** option specifies how many extended sessions are allowed for the protocol port, and can be 1-255.

[no] lsn-rule-list destination *list-name*

Matches traffic based on destination IP address, traffic type, or protocol port, in addition to matching on the source IP addresses in the class list that uses this LID.

If traffic matches both a source IP address in the class list and a destination address, traffic type, or protocol port in the rule list, the action specified in the rule list is applied to the traffic.

(To configure an LSN rule list, see "lsn-rule-list" on page 482.)

[no] name *string*

Assigns a name to the LID.

[no] override {drop | pass-through}

Overrides NAT for matching traffic, and performs the specified action instead:

drop – Drops the traffic.

pass-through – Forwards the traffic without performing NAT.

[no] respond-to-user-mac

Enables MAC-based nexthop routing. When MAC-based nexthop routing is enabled, the AX device sends the reply to an inside client's request back through the same route hop on which the request was received. The AX device identifies the route hop based on its MAC address. The AX device sends the reply to the MAC address, instead of using the route table to select the next hop for the reply.

`[no] source-nat-pool pool-name`

Binds an LSN NAT pool to the LID.

`[no] user-quota {tcp | udp | icmp} quota-num [reserve reserve-num]`

Configures the per-user mapping quota for the specified protocol. The *quota-num* option specifies the maximum number of sessions allowed per client and can be 1-64000.

The **reserve** option allows you to specify how many ports to reserve on a NAT IP for each user, 0-64000. If unspecified, the reserve value is the same as the user-quota value.

Default

The LSN LID options have the following default values:

- **drop-on-nat-pool-mismatch –** not set
- **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

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).

```
AX(config)#lsn-lid 5
AX(config-lsn lid)#source-nat-pool LSN_POOL1
AX(config-lsn lid)#user-quota tcp 100
AX(config-lsn lid)#user-quota udp 300 reserve 100
AX(config-lsn lid)#user-quota icmp 10
AX(config-lsn lid)#extended-user-quota tcp service-port 25 sessions 3
```

Example The following commands configure an LSN LID in which MAC-based nex-thop routing is enabled:

```
AX(config)#lsn-lid 1
AX(config-lsn lid)#respond-to-user-mac
AX(config-lsn lid)#exit
```

Example The following commands configure a class list that maps inside clients to the LSN LID:

```
AX(config)#class-list mac-reply-clients
AX(config-class list)#192.168.0.0 /16 lsn-lid 1
```

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.

Note: You also can use LSN rule lists for NAT64 and DS-Lite.

Syntax `[no] lsn-rule-list list-name`

Parameter	Description
list-name	Name of the rule list.

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

Command	Description

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

[**no**] **default**

Enters the configuration level for the default set of rules. The default set of rules is used for traffic that does not exactly match an IP host or subnet rule. (See below.)

[**no**] **domain-name** *string*

Enters the configuration level for the set of rules to apply to the specified domain name.

[**no**] [*ipv4addr* {*/mask-length* | *subnet-mask*}]

Enters the configuration level for the set of rules to apply to the specified IP host address or subnet.

Either command changes the CLI to the configuration level for the specified rule list, where the following commands are available.

[**no**] **icmp action** *action* | **no-action**

Performs the specified action on matching ICMP traffic. See the section for *action* and **no-action** below.

[**no**] **others action** *action* | **no-action**

Performs the specified action on matching traffic of types other than ICMP, TCP, or UDP. See *action* below.

[**no**] {**tcp** | **udp**} **port** {**any** | *portnum* [**to** *portnum*]} **action** *action* | **no-action**

Performs the specified action on matching traffic with the specified TCP or UDP port(s).

action

Specifies the action to perform on matching traffic:

drop – Drops the traffic.

nat pool {*pool-name* | *pool-group-name*} – 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.

`pass-through` – Forwards the traffic without performing NAT.

`template http-alg` – Processes traffic based on the specified HTTP-ALG template. (See “ip nat template http-alg” on page 477.)

`Note:` 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.)

`no-action` Excludes matching traffic from the actions in the rule list, but still performs NAT for the traffic. (For more information, see the *AX Series 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. (See “lsn-rule-list” on page 482.)

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. Instead, the traffic is dropped and the LSN Rule-List NAT Pool Mismatch Drop counter in **show ip nat lsn statistics** output is incremented.

Default and IP-specific Rules

In an LSN rule list, you can configure the following types of rules:

- Rules for specific IP addresses or subnets
- 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.)

LSN Show Commands

This section describes the show commands for LSN.

show ip nat lsn alg

Description

Show Application Level Gateway (ALG) information for LSN, NAT64, and DS-Lite.

Syntax

```
show ip nat lsn alg
{esp | ftp | pptp | rtsp | sip | tftp}
{config | statistics [debug]}
```

Parameter	Description
`esp | ftp | pptp | rtsp | sip | tftp`	Specifies the protocol: **esp** – IPsec Encapsulating Security Payload (ESP) **ftp** – File Transfer Protocol (FTP) **pptp** – Point-to-Point Tunneling Protocol (PPTP) Generic Routing Encapsulation (GRE) **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 ALG information for FTP:

```
AX#show ip nat lsn alg ftp config
LSN ALG for FTP is enabled on port 21.
AX#show ip nat lsn alg ftp statistics
LSN FTP ALG Statistics:
---------------------------
Port Mode (PORT) Requests From Client    3
Passive Mode (PASV) Replies From Server  1
```

Example The following command shows statistics for FTP ALG:

```
AX#show ip nat 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
```

Table 3 describes the fields in the command's output.

TABLE 3 show ip nat lsn alg ftp statistics fields

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 RTSP ALG:

```
AX#show ip nat 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
```

Table 4 describes the fields in the command's output.

TABLE 4 show ip nat lsn alg rtsp statistics fields

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 AX device was out of 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 AX device was out of memory for sessions.

Example

The following command shows statistics for SIP ALG:

```
AX#show ip nat 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
```

Table 5 describes the fields in the command’s output.

TABLE 5 show ip nat lsn alg sip statistics fields

Field	Description
SIP Method REGISTER	Number of SIP REGISTER messages received by the AX 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 AX device.
SIP Method ACK	Number of SIP ACK messages received by the AX device.
SIP Method CANCEL	Number of SIP CANCEL messages received by the AX device.
SIP Method BYE	Number of SIP BYE messages received by the AX device.
SIP Method OPTIONS	Number of SIP OPTIONS messages received by the AX device.
SIP Method PRACK	Number of SIP PRACK messages received by the AX device.
SIP Method SUBSCRIBE	Number of SIP SUBSCRIBE messages received by the AX device.

TABLE 5 show ip nat lsn alg sip statistics fields (Continued)

Field	Description
SIP Method NOTIFY	Number of SIP NOTIFY messages received by the AX device.
SIP Method PUBLISH	Number of SIP PUBLISH messages received by the AX device.
SIP Method INFO	Number of SIP INFO messages received by the AX device.
SIP Method REFER	Number of SIP REFER messages received by the AX device.
SIP Method MESSAGE	Number of SIP MESSAGE messages received by the AX device.
SIP Method UPDATE	Number of SIP UPDATE messages received by the AX device.
SIP Method UNKNOWN	Number of SIP UNKNOWN messages received by the AX device.

Example

The following command shows statistics for TFTP ALG:

```
AX#show ip nat lsn alg tftp statistics
LSN TFTP ALG Statistics:
---------------------------
TFTP Client Sessions Created              2
```

The counter indicates the number of UDP sessions created by clients to destination port 69.

show ip nat lsn full-cone-sessions

Description

Show currently active LSN full-cone sessions.

Syntax

```
show ip nat lsn full-cone-sessions
[brief]
[inside-user ipaddr]
[pool pool-name]
```

Parameter	Description
brief	Displays only statistics.
inside-user *ipaddr*	Displays full-cone sessions only for the specified user.

pool *pool-name* Displays only the full-cone sessions that use a public IP address from the specified LSN NAT pool.

Mode

All

Example

The following command shows currently active LSN full-cone sessions:

```
AX#show ip nat lsn full-cone-sessions
LSN Full Cone Sessions:
Prot Inside Address                  NAT Address                 Conns    Pool              CPU  Age
---------------------------------------------------------------------------------------------------
TCP  192.168.1.1:20001               203.0.113.1:20001            1        pool1              1    2
TCP  192.168.2.1:30001               203.0.113.1:30001            1        pool1              4    11
TCP  192.168.255.1:50001             203.0.113.1:50001            1        pool1              13   15
Total Full Cone Sessions: 3
```

Table 6 describes the fields in the command’s output.

TABLE 6 show ip nat lsn full-cone-sessions fields

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.
Conns	Number of connections currently using the session.
Pool	LSN NAT pool from which the public IP address was assigned.
CPU	AX CPU on which the session resides.
Age	Number of seconds the session has been in effect.
Statistics (brief option)	
LSN TCP Full-cone Session Created	Number of TCP full-cone sessions created.
LSN TCP Full-cone Session Freed	Number of TCP full-cone sessions freed.
LSN UDP Full-cone Session Created	Number of UDP full-cone sessions created.
LSN UDP Full-cone Session Freed	Number of UDP full-cone sessions freed.
LSN Full-cone Session Creation Failed	Number of times an attempt to create an LSN full-cone session failed.

show ip nat lsn inside-user

Description

Show session information for a specific LSN inside client.

Syntax

show ip nat lsn inside-user *ipaddr*

Parameter	Description
ipaddr	Specifies the inside IP address of the user.

Mode

All

Example

The following command shows LSN session information for LSN user 10.10.10.100:

```
AX#show ip nat lsn inside-user 10.10.10.100
LSN User-Quota Sessions:
Inside Address       NAT Address          ICMP   UDP    TCP    Pool             LID
-------------------------------------------------------------------------------------
10.10.10.100         172.7.7.30           0      3      2      lsn0             1
Total User-Quota Sessions Shown: 1

LSN Full Cone Sessions:
Prot Inside Address         NAT Address            Conns  Pool             CPU Age
-------------------------------------------------------------------------------------
UDP  10.10.10.100:9385      172.7.7.30:42025       0      lsn0             1   120
UDP  10.10.10.100:47967     172.7.7.30:23583       1      lsn0             1   -
UDP  10.10.10.100:62210     172.7.7.30:52226       1      lsn0             4   -
TCP  10.10.10.100:28483     172.7.7.30:33795       1      lsn0             1   -
TCP  10.10.10.100:28482     172.7.7.30:29698       1      lsn0             2   -
Total Full Cone Sessions: 5

LSN Data Sessions:
Prot Forward Source        Forward Dest          Reverse Source        Reverse Dest          Age
Hash Flags
--------------------------------------------------------------------------------------------------
--------------
Udp  10.10.10.100:47967    172.7.7.100:5300      172.7.7.100:5300      172.7.7.30:23583      300
1    NF
Tcp  10.10.10.100:28483    172.7.7.100:80        172.7.7.100:80        172.7.7.30:33795      0
1    NF
Tcp  10.10.10.100:28482    172.7.7.100:80        172.7.7.100:80        172.7.7.30:29698      0
2    NF
Udp  10.10.10.100:62210    172.7.7.100:5300      172.7.7.100:5300      172.7.7.30:52226      300
4    NF
```

Table 7 describes the fields in the command’s output.

TABLE 7 show ip nat lsn inside-user fields

Field	Description
LSN User-Quota Sessions	Lists the following user-quota session information for the user: • Inside Address – IPv4 address of the client • NAT Address – Client IPv4 NAT address from the LSN pool on the AX 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
LSN Full-Cone Sessions	Lists the following information for the user’s full-cone session: • Prot – Protocol of the session • Inside Address – IPv4 address of the client • NAT Address – Client IPv4 NAT address from the LSN pool on the AX device • Conns – Number of connections currently using the session • Pool – LSN NAT pool from which the NAT address for the session was selected • CPU – AX CPU on which the session resides • Age – Number of seconds the session has been in effect
LSN Data Sessions	Lists the following data session information for the user: • Prot – Protocol of the session • Forward Source – IPv4 address and protocol port of the client • Forward Dest – IPv4 address and protocol port of the server • Reverse Source – IPv4 address and protocol port of the server • Reverse Dest – Client IPv4 NAT address from the LSN pool on the AX device • 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 ip nat lsn pool-statistics

Description

Show LSN pool statistics.

Syntax

```
show ip nat lsn pool-statistics
[brief]
[misc]
[peaks]
[pool pool-name]
[top num
  {used | used-icmp | used-udp | used-tcp |
   reserved | reserved-udp | reserved-tcp |
   users}]
```

Parameter	Description
brief	Displays fewer details.
misc	Displays miscellaneous per-IP information.
peaks	Displays peak statistics.
pool *pool-name*	Displays statistics only for the specified pool.
top *num type*	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. **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.

Mode All

Example The following command shows LSN pool statistics:

```
AX#show ip nat lsn pool-statistics
LSN Address Pool Statistics:
----------------------------
pool1   Address        Users  ICMP   Freed  Total  UDP    Freed  Total  Rsvd   TCP    Freed  Total  Rsvd
--------------------------------------------------------------------------------------------------------
        203.0.113.1    0      0      0      0      0      0      0      0      0      0      0      0
        203.0.113.2    0      0      0      0      0      0      0      0      0      0      0      0
        203.0.113.3    0      0      0      0      0      0      0      0      0      0      0      0
```

Table 8 describes the fields in this command’s output.

TABLE 8 show ip nat lsn pool-statistics fields

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.
TCP	Number of TCP ports currently in use.
Freed (TCP)	Total number of TCP ports freed.
Total (TCP)	Total number of TCP ports allocated. TCP column + Freed column = Total column.
Rsvd (TCP)	Total of all TCP reserve settings for each user that is currently using the NAT IP address. For example, if an LID has the setting “user-quota tcp 100 reserve 60”, and there are 10 users using the LID d on the NAT IP address, the Rsvd value is 10*60 = 600.

show ip nat lsn port-overloading config

Description Display the configured Port Overloading settings that are ready to be deployed.

Syntax **`show ip nat lsn port-overloading config`**

Mode All

show ip nat lsn port-reservations

Description Show static LSN port reservations.

Syntax **`show ip nat lsn port-reservations`**

Mode All

Example The following command shows static LSN port reservations:

```
AX#show ip nat 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
```

Table 9 describes the fields in this command’s output.

TABLE 9 show ip nat lsn port-reservations fields

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 ip nat lsn radius server

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

Syntax

```
show ip nat lsn radius server
{config | statistics}
```

Parameter	Description
`config`	Displays the configuration for the AX RADIUS server.
`statistics`	Displays statistics for the AX RADIUS server.

Mode All

Introduced in Release 2.6.6-P4

show ip nat lsn radius table

Description Show the RADIUS accounting information stored on the AX device.

Syntax

```
show ip nat lsn radius table
[
brief |
inside-ip ipaddr |
msisdn num |
imsi num |
imei num
]
```

Parameter	Description
`brief`	Shows statistics only.
`inside-ip` *`ipaddr`*	Shows entries only for inside IP addresses.
`msisdn` *`num`*	Shows entries only for MSIDSN numbers.
`imsi` *`num`*	Shows entries only for IMSI numbers.
`imei` *`num`*	Shows entries only for IMEI numbers.

Mode All

Introduced in Release 2.6.6-P4

show ip nat lsn statistics

Description Show LSN statistics.

Syntax `show ip nat lsn statistics [others]`

Parameter	Description
others	Displays a set of error statistics that are not included in the standard display. (See example below.)

Mode All

Example The following command shows LSN statistics:

```
AX#show ip nat 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
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
NAT Pool Mismatch Drop                   0
TCP Port Overloaded                      0
UDP Port Overloaded                      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 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
```

Table 10 describes the fields in this command’s output.

TABLE 10 show ip nat lsn statistics fields

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 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.

TABLE 10 show ip nat lsn statistics fields (Continued)

Field	Description
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.
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.

TABLE 10 show ip nat lsn statistics fields (Continued)

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.
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.
UDP Port Overloading Session Freed	Number of times a session created on an overloaded UDP port was freed.
NAT IP TCP Max Ports Allocated	Maximum number of NAT IP TCP ports allocated.
NAT IP UDP Max Ports Allocated	Maximum number of NAT IP UDP ports allocated.

TABLE 10 show ip nat lsn statistics fields (Continued)

Field	Description
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 NAT-ted.

show ip nat lsn system-status

Description Show system-level information for LSN.

Syntax **show ip nat lsn system-status**

Mode All

Example The following command shows system-level information for LSN:

```
AX#show ip nat 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 Pool Usage:
---------------
TCP NAT Pool Used: 0
TCP NAT Pool Free: 0
UDP NAT Pool Used: 0
UDP NAT Pool Free: 0
```

Table 11 describes the fields in the command’s output.

TABLE 11 show ip nat lsn system-status fields

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 data sessions.
NAT Pool Usage	Shows usage and availability for LSN NAT pools.

show ip nat lsn user-quota-sessions

Description

Show LSN user-quota session information.

Syntax

```
show ip nat lsn user-quota-sessions
[brief]
[inside-user ipaddr]
[pool pool-name]
[top num {all | icmp | tcp | udp}]
```

Parameter	Description
brief	Displays only session statistics.
inside-user *ipaddr*	Displays session information only for the specified user IP address.
pool *pool-name*	Displays session information only for the specified LSN NAT pool.
top *num type*	Limits the display to the sessions with the highest counters for the specified resource type. You can specify 1-100.

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

Table 12 describes the fields in the command's output.

TABLE 12 show ip nat lsn user-quota-sessions fields

Field	Description
Information for Individual Sessions:	
Inside Address	Inside client's IP address.
NAT Address	Public IP address assigned to the client by LSN.
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	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.
Statistics (brief option)	
LSN User-Quota Created	Number of port mappings created for which the user quota had available mappings.
LSN User-Quota Freed	Number of port mappings that were created for which the user quota had available mappings, that were later freed.
LSN User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
LSN TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
LSN UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
LSN ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
LSN Extended User-Quota Matched	Number of times the extended user quota was used to create a mapping.

TABLE 12 show ip nat lsn user-quota-sessions fields (Continued)

Field	Description
LSN Extended User-Quota Exceeded	Number of times a NAT port was unavailable to a client because the client had exceeded the extended user quota.
LSN Data Session User-Quota Exceeded	Number of times a client exceeded their data session quota.

show lsn-lid

Description Show information for Limit IDs (LIDs) for Large Scale NAT (LSN).

Syntax

```
show lsn-lid [num]
```

Mode All

show lsn-rule-list

Description Show information for LSN rule lists.

Syntax

```
show lsn-rule-list list-name [statistics]
```

Mode All

Config Commands: Port Control Protocol

The commands in this chapter configure Port Control Protocol (PCP).

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Notes About the Current Release

- PCP is in Beta form and conforms to parts of IETF drafts 12 and 13. PCP in this release is intended for non-production testing purposes only.
- 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).
- In this release, the “Reserved” fields are not zeroed out. Clients should ignore these fields and not check the contents of them. In future releases, these fields will be set to zero.

PCP Configuration Commands

This section describes the PCP configuration commands.

ip nat pcp default-template

Description

Specify the Port Control Protocol (PCP) template to use as the set of default PCP settings.

Syntax

```
[no] ip nat pcp default-template template-name
```

Parameter	Description
template-name	Name of the PCP template. (To configure a PCP template, see "ip nat template pcp" on page 506.)

Default

PCP is disabled by default. To enable it, configure a PCP template, then activate it on a global basis using the **ip nat pcp default-template** command.

Mode

Configuration mode

Usage

When PCP is enabled, the AX device acts as a PCP server for Large Scale NAT (LSN) clients (PCP clients). The AX 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 AX device then sends a PCP response message back to the PCP client. The mapping created for the client is an implicit dynamic mapping.

ip nat template pcp

Configure a template to set Port Control Protocol (PCP) options.

Syntax

```
[no] ip nat template pcp template-name
```

Parameter	Description
template-name	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. See "Config Commands: Global" on page 79.)

Command	Description
`[no] allow-third-party`	Enables support for the third-party option in MAP requests. This option instructs the AX 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.
`[no] draft-version {12 | 13}`	Specifies the PCP draft version to support. **12** – IETF draft-ietf-pcp-base-12 **13** – IETF draft-ietf-pcp-base-13
`[no] max-life-time` *minutes*	Specifies the maximum lifetime of PCP mappings. You can specify 1-1440 minutes.
`[no] pcp-udp-port` *portnum*	Specifies the UDP destination port for PCP.

Default

PCP disabled by default. To enable it, use this command to configure a PCP template, then use the **ip nat pcp default-template** command to activate it ("ip nat pcp default-template" on page 506).

The template options have the following default settings:

- **allow-third-party** – disabled
- **draft-version** – 13
- **max-life-time** – 5
- **pcp-udp-port** – 5351

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).

In the current release, PCP conforms to parts of IETF draft 13 and is intended for non-production testing purposes only.

PCP Show Commands

This section describes the show commands for PCP.

show ip nat pcp statistics

Description

Shows statistics for Port Control Protocol (PCP).

Syntax

```
show ip nat pcp statistics
```

Mode

All

Example

The following command shows PCP statistics:

```
AX#show ip nat pcp statistics
Traffic statistics for PCP:
---------------------------
Received packet is not a PCP request     0
Invalid PCP opcode                       0
No route for PCP response                0
PCP request is not IP                    0
Egress port for PCP response down        0
LSN TCP fullcone session alloc failure   0
LSN UDP fullcone session alloc failure   0
LSN OTHER fullcone session alloc failure 0
DSLITE TCP fullcone session alloc failure 0
DSLITE UDP fullcone session alloc failure 0
DSLITE OTHER fullcone session alloc failure 0
NAT64 TCP fullcone session alloc failure 0
NAT64 UDP fullcone session alloc failure 0
NAT64 OTHER fullcone session alloc failure 0
LSN TCP fullcone session alloc success   1
LSN UDP fullcone session alloc success   0
LSN OTHER fullcone session alloc success 0
DSLITE TCP fullcone session alloc success 0
DSLITE UDP fullcone session alloc success 0
DSLITE OTHER fullcone session alloc success 0
NAT64 TCP fullcone session alloc success 0
NAT64 UDP fullcone session alloc success 0
NAT64 OTHER fullcone session alloc success 0
Malformed request                        0
Unsupported version                      0
```

```
Client address mismatch                   0
Malformed options                         0
Third_party_option_disallowed             0
Unsupported options                       0
User quota exceeded                       0
Cannot provide ext port                   0
Request processing success                1
```

Table 13 describes the fields in the command’s output.

TABLE 13 show ip nat pcp statistics fields

Field	Description
Received packet is not a PCP request	Number of PCP requests in which the request bit was not set to 0.
Invalid PCP opcode	Number of PCP requests in which the OpCode was incorrect.
No route for PCP response	Number of times the AX device did not have a return route. (No full-cone session was created.)
PCP request is not IP	Number of times the AX interface received a PCP request with an unexpected Layer 3 protocol.
Egress port for PCP response down	Number of times the AX interface needed for sending a PCP response to a client was down.
LSN TCP fullcone session alloc failure	Number of times allocation of an LSN full-cone session for TCP failed.
LSN UDP fullcone session alloc failure	Number of times allocation of an LSN full-cone session for UDP failed.
LSN OTHER fullcone session alloc failure	Number of times allocation of an LSN full-cone session for other traffic types failed.
DSLITE TCP fullcone session alloc failure	Number of times allocation of a DS-Lite full-cone session for TCP failed.
DSLITE UDP fullcone session alloc failure	Number of times allocation of a DS-Lite full-cone session for UDP failed.
DSLITE OTHER full-cone session alloc failure	Number of times allocation of a DS-Lite full-cone session for other traffic types failed.
NAT64 TCP full-cone session alloc failure	Number of times allocation of a NAT64 full-cone session for TCP failed.

TABLE 13 show ip nat pcp statistics fields (Continued)

Field	Description
NAT64 UDP fullcone session alloc failure	Number of times allocation of a NAT64 full-cone session for UDP failed.
NAT64 OTHER fullcone session alloc failure	Number of times allocation of a NAT64 full-cone session for other traffic types failed.
LSN TCP full-cone session alloc success	Number of LSN full-cone sessions successfully allocated for TCP.
LSN UDP full-cone session alloc success	Number of LSN full-cone sessions successfully allocated for UDP.
LSN OTHER fullcone session alloc success	Number of LSN full-cone sessions successfully allocated for other traffic types.
DSLITE TCP fullcone session alloc success	Number of DS-Lite full-cone sessions successfully allocated for TCP.
DSLITE UDP fullcone session alloc success	Number of DS-Lite full-cone sessions successfully allocated for UDP.
DSLITE OTHER full-cone session alloc success	Number of DS-Lite full-cone sessions successfully allocated for other traffic types.
NAT64 TCP full-cone session alloc success	Number of NAT64 full-cone sessions successfully allocated for TCP.
NAT64 UDP fullcone session alloc success	Number of NAT64 full-cone sessions successfully allocated for UDP.
NAT64 OTHER fullcone session alloc success	Number of NAT64 full-cone sessions successfully allocated for other traffic types.
Malformed request	Number of times the AX device sent an “Malformed request” response code in response to a PCP request, per the PCP specification.
Unsupported version	Number of times the AX device sent an “Unsupported version” response code in response to a PCP request, per the PCP specification.
Client address mismatch	Number of times a PCP client’s IP address and protocol port in the PCP request header did not match the source IP address and protocol port of the PCP request packet.
Malformed options	Number of times the AX device sent an “Malformed Option” response code in response to a PCP request, per the PCP specification.

TABLE 13 show ip nat pcp statistics fields (Continued)

Field	Description
Third_party_ option_ disallowed	Number of times a third-party request was received but was not allowed because the option was disabled in the active PCP template.
Unsupported options	Number of times the AX device sent an “Unsupported Option” response code in response to a PCP request, per the PCP specification.
User quota exceeded	Number of times a full-cone session was not allocated for a client because doing so would result in exceeding the client’s user quota.
Cannot provide ext port	Number of times the AX device could not allocate an external port to a client
Request processing success	Number of times a valid request was successfully processed.

Config Commands: NAT64 / DNS64

The commands in this chapter configure global settings for NAT64 / DNS64.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

DNS64 Configuration Commands

This section describes the DNS64 configuration commands.

ip nat pool (for DNS64)

Description

Configure an IPv4 pool, for DNS64 to use while acting as a proxy for a local IPv4 DNS server.

Syntax

```
[no] ip nat pool pool-name
start-ipaddr end-ipaddr
netmask {subnet-mask | /mask-length}
[gateway ipaddr]
[ha-group-id group-id [ha-use-all-ports]]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | /*mask-length*}	Network mask for the IP addresses in the pool.
gateway *ipaddr*	Default gateway to use for NATted traffic.
ha-group-id *group-id* [**ha-use-all-ports**]	HA group ID, 1-31. The **ha-use-all-ports** option disables division of the pool's ports between AX devices. Without this option, the AX device automatically allocates half of each pool address's ports to one of the AX devices and allocates the other half of the ports to the other AX device. (See "Usage" below.)

Default

None

Mode

Configuration mode

Usage

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.

For conditions under which the NAT gateway is needed, if no NAT gateway is configured, the AX device uses the default gateway configured for the AX device's other traffic instead.

The command also has an **lsn** option (not shown above). This option is applicable to NAT64 but is not applicable to DNS64. (For NAT64 pool configuration, see "ip nat pool (for NAT64)" on page 528.)

Port Allocation Between AX Devices in High Availability Deployments (ha-use-all-ports option)

By default, when you assign an IP NAT pool to an HA group, the AX device automatically allocates half of each pool address's ports to one of the AX devices and allocates the other half of the ports to the other AX device.

This automatic allocation is used to prevent simultaneous use of the same port number by both AX devices. For example, without this protection, it would be possible for the same IP address and protocol port number to be in use on both AX devices in an Active-Active configuration.

However, this protection also requires the pool to be configured with more addresses than will actually be needed.

In some cases, there is no benefit to dividing the pool's ports between the AX devices. In particular, there is no benefit for DNS virtual ports. DNS sessions are very short-lived and are never synchronized between the AX devices. For this reason, there is no risk that the same NAT port will be in use on more than one session at the same time. You can use the **ha-use-all-ports** option to disable division of the ports between AX devices.

Note: It is recommended to use the **ha-use-all-ports** option only for DNS virtual ports. Using this option with other virtual port types is not valid.

ip nat pool-group (for DNS64)

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
[ha-group-id group-id]
```

Parameter	Description
pool-group-name	Name of the pool group.
ha-group-id *group-id*	HA group ID, 1-31.

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. See "Config Commands: Global" on page 79.)

Parameter	Description
member *pool-name*	Name of a configured IP address pool.

Default None

Mode Configuration mode

Usage To use a non-contiguous range of addresses, configure a separate pool for each contiguous portion of the range, then configure a pool group that contains the pools.

The addresses within an individual pool still must be contiguous, but you can have gaps between the ending address in one pool and the starting address in another pool. You also can use pools that are in different subnets.

For Large Scale NAT (LSN), a pool group can contain up to 25 pools. For other types of NAT, a pool group can contain up to 5 pools. Pool group members must belong to the same protocol family (IPv4 or IPv6) and must use the same HA ID. A pool can be a member of multiple pool groups.

If a pool group contains pools in different subnets, the AX 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 AX selects the pool that is in the subnet for the outbound route.

The AX 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:

```
AX(config)#ip nat pool-group group1
AX(config-pool-group)member pool1
AX(config-pool-group)member pool2
AX(config-pool-group)member pool3
```

ipv6 nat pool (for DNS64)

Description

Configure an IPv6 pool, for DNS64 to use while acting as a proxy for a local IPv6 DNS server.

Syntax

```
[no] ipv6 nat pool pool-name
start-ipv6-addr end-ipv6-addr
netmask mask-length
[gateway ipaddr]
[ha-group-id group-id]
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask *mask-length*	Network mask for the IP addresses in the pool, 64-128.
gateway *ipv6-addr*	Next-hop gateway address.
ha-group-id *group-id*	HA group ID, 1-31.

Default

None

Mode

Configuration mode

Usage

For more information about the **gateway** and **ha-group-id** options, see “ip nat pool (for DNS64)” on page 513.

The command also has an **lsn** option (not shown above). This option is applicable to NAT64 but is not applicable to DNS64. (For NAT64 pool configuration, see “ip nat pool (for NAT64)” on page 528.)

If both IPv4 and IPv6 local DNS servers will be proxied, you also need to configure an IPv6 ACL. The ACL directs IPv6 traffic to the IPv6 pool instead of the IPv4 pool. (See “ipv6 access-list” on page 266.)

nat64 prefix

Description Configure the NAT64 prefix.

Syntax

```
[no] nat64 prefix
{ipv6-addr/nn | well-known}
[inside source class-list list-name]
[ha-group-id group-id]
```

Parameter	Description
ipv6-addr/nn	Specifies the prefix.
well-known	Sets the prefix to the well-known (standard) value, 64:ff9b::/96.
inside source class-list *list-name*	Specifies a class list of inside source parameters for the prefix.
ha-group-id *num*	Assigns the prefix to a High Availability (HA) group. You can specify 1-31.

Default The default is **well-known**. No HA group or class list is assigned by default.

Mode Configuration mode

slb server

Description Configure the local DNS server to be proxied.

Syntax

```
[no] slb server server-name {ipaddr | ipv6-addr}
```

This command creates the server and changes the CLI to the configuration level for the server, where the following commands are available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[**no**] **health-check** [*monitor-name*]	Enables health monitoring of the port. The *monitor-name* specifies the name of a configured health monitor.

If you omit this command or you enter it without the *monitor-name* option, the default Layer 3 (ICMP) health monitor is used:

`[no] port` *`port-num`* **`udp`**

Specifies the UDP port on which the server listens for DNS traffic.

`disable | enable` – Disables or re-enables the port.

`[`**`no`**`]` **`health-check`** `[`*`monitor-name`*`]` `[`**`follow-port`** *`port-num`*`]`– Enables health monitoring for a server.. The *monitor-name* option specifies the name of a configured health monitor.

The **follow-port** *port-num* option specifies another real port upon which to base this port's health status. Both the real port and the port to use for the real port's health status must be the same type, TCP or UDP. By default, this option is not set.

If you omit the **health-check** command or you enter it without the *monitor-name* option, the default UDP health monitor is used. (See below.)

`stats-data-disable | stats-data-enable` – Disables or enables statistical data collection for the port.

`Note:` The other configuration commands are not applicable to DNS64 / NAT64.

Default None

Mode Configuration mode

Usage The normal form of the **slb 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. The AX Series supports both address formats.

Default Health Monitoring

The following health monitors are enabled by default.

- ICMP – Server health check. Every 5 seconds, the AX 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 AX device.

If the server does not reply after the fourth attempt (the first attempt followed by 3 retries), the AX device sets the server state to DOWN.

- UDP – Protocol port health check. Every 5 seconds, the AX 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.

slb service-group

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

Syntax `[no] slb service-group group-name udp`

Parameter	Description
group-name	Name of the group, 1-31 characters.

This command changes the CLI to the configuration level for the specified service-group, where the following command is available:

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] member *server-name*:*portnum* **[disable | enable] [priority** *num*] **[template** *template-name*] **[stats-data-disable | stats-data-enable]**	Adds the local DNS server and port to the service group. *server-name*:*portnum* – Server name and UDP port number on the server. **disable | enable** – Disables or re-enables the server and port, for this service group only. **priority** *num* – Sets the preference for this server and port, 1-16.

`stats-data-disable` – Disables statistical data collection for the service-group member.

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.

slb template dns

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

Syntax

```
[no] slb 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 command is available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
`[no] dns64 [options]`	Enables DNS64 and configures DNS64 options. **`answer-only`** – Synthesizes IPv6 addresses for only the resource records in the ANSWER section of DNS replies. If you disable this option, the IPv4 addresses in all other sections of DNS replies are synthesized to IPv6 too. **`auth-data`** – When the AX 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. **`cache`** – Uses a cached A-query response to provide AAAA query responses for the same hostname, without consulting the DNS server. 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 AX

device does not consult the DNS server. Instead, the AX device uses the cached type A answer to synthesize a AAAA response, and sends the synthesized response to the client.

`change-query` – When the AX 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 AX device does not need to wait for an error or empty response, or for the response to time out.

`compress` – Saves network costs by compressing DNS packets.

`deep-check-rr drop-cname` – 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.

`ignore-rcode3` – Ignores any DNS response with rcode 3 in response to a AAAA query. The AX 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.

`max-qr-length` *`num`* – Forwards the response from the DNS server to the client without any modification to the response, if the question-record length is greater than the specified length. The length can be 1-1023 bytes.

`parallel-query` – Sends both an IPv6 AAAA request and an IPv4 A request in parallel (at the same time) on behalf of the client. When this option is enabled, the AX 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 AX device forwards the last invalid response to the client.

Note: It is recommended to disable the **passive-query** option and enable the **single-response** option when using the **parallel-query** option.

passive-query – Initiates an A query upon receiving an empty response or error for a AAAA query.

retry – Specifies the maximum number of times the AX 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.

single-response – When the AX device is operating in parallel-query mode, the AX device will send two queries to the DNS server at the same time. Both queries could come back with valid responses.

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 AX device will forward both responses to the server, if both responses are valid.

timeout *seconds* – Specifies the maximum number of seconds the AX device waits for a AAAA response before sending an A query. You can specify 1-15 seconds.

trans-ptr – 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 AX device, the response is synthesized and sent back to the client as if it were a response for the synthesized IPv6 address.

ttl *seconds* – Specifies the maximum TTL to use in synthesized AAAA replies, in place of the TTL value in the original IPv4 DNS reply.

– If the TTL value in the template is lower than the TTL value in the IPv4 reply, the template's TTL value is used in the synthesized IPv6 reply.

– If the TTL value in the template is equal to or higher than the TTL value in the IPv4 reply, the TTL value in the IPv4 reply is used in the synthesized IPv6 reply.

You can specify 0-15.

Default

DNS64 is disabled by default. When you enable it, the DNS64 options have the following defaults:

- **answer-only** – enabled
- **auth-data** – disabled
- **cache** – disabled
- **change-query** – disabled
- **compress** – enabled
- **deep-check-rr** – disabled
- **ignore-rcode3** – enabled
- **max-qr-length** – 128
- **parallel-query** – disabled
- **passive-query** – enabled
- **retry** – 3
- **single-response** – enabled
- **timeout** – 1
- **trans-ptr** – disabled
- **ttl** – not set

Mode

Configuration mode

slb virtual-server

Description

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

Syntax

```
[no] slb virtual-server name {ipaddr | ipv6-addr}
```

This command creates the server and changes the CLI to the configuration level for the virtual server, where the following commands are available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
`[no] access-list name acl-name source-nat-pool {pool-name | pool-group-name}`	Binds the virtual port to an IPv6 ACL and IPv6 source NAT pool.
`[no] port port-number dns-udp`	Specifies the UDP port number and the port type, **dns-udp**. This command changes the CLI to the configuration level for the port, where the following commands are available.
`[no] service-group group-name`	Binds the virtual port to the service group.
`[no] source-nat pool {pool-name | pool-group-name}`	Binds the virtual port to an IP address pool or pool group.
`[no] template dns template-name`	Binds the virtual port to the DNS template containing the DNS64 settings. (See “slb template dns” on page 521.)

`[no] template policy` *`template-name`*	Binds the virtual port to a policy template, if applicable. (See "slb template policy" on page 537.)

Default None

Mode Configuration mode

NAT64 Configuration Commands

This section describes the NAT64 configuration commands.

class-list (for NAT64)

Description Configure a class list that specifies IPv6 addresses or prefixes on which to perform an override action. For matching entries, the override action is applied instead of the configured NAT64 action.

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a standalone file on the AX device.

Note: A class list can be exported only if you use the **file** option.

This command changes the CLI to the configuration level for the specified class list, where the following command is available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
`[no] ipv6-addr/prefix {glid | lid | lsn-lid} num`	Adds an entry to the class list. *ipv6-addr/prefix* – Specifies an IPv6 address or prefix on which to perform an override action **{glid | lid}** *num* – Specifies a Global Limit ID (GLID) or a Limit ID (LID) configured in a policy template. These options apply only to NAT64 override. **lsn-lid** *num* – Specifies the LID that refers to the NAT pool (or group of pools) containing the IPv4 address(es) to use for NATting traffic from IPv6 clients to IPv4 servers.

Default None

Mode Configuration mode

Usage If you plan to use a GLID, see "glid (for NAT64 override)" on page 529. If you plan to use a policy template instead, see "slb template policy" on page 537.

ip nat outside

Description Enable IPv4 outside NAT on the interface connected to the IPv4 Internet.

Syntax

```
[no] ip nat outside
```

Default Disabled

Mode Interface configuration level

ipv6 nat inside

Description Enable IPv6 inside NAT on the interface connected to the IPv6 clients.

Syntax

```
[no] ipv6 nat inside
```

Default Disabled

Mode Interface configuration level

ip 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.

Syntax

```
[no] ip nat pool pool-name
start-ipaddr end-ipaddr
netmask {subnet-mask | /mask-length} lsn
```

Parameter	Description
pool-name	Name of the address pool.
start-ipaddr	Beginning (lowest) IP address in the range.
end-ipaddr	Ending (highest) IP address in the range.
netmask {*subnet-mask* | */mask-length*}	Network mask for the IP addresses in the pool.
gateway *ipaddr*	Default gateway to use for NATted traffic.
ha-group-id *group-id* [**ha-use-all-ports**]	HA group ID, 1-31. The **ha-use-all-ports** option disables division of the pool’s ports between AX devices. Without this option, the AX device automatically allocates half of each pool address’s ports to one of the AX devices and allocates the other half of the ports to the other AX device. (See “Usage” in “ip nat pool (for DNS64)” on page 513.)
lsn	Indicates that the pool is for NAT64. This option is required.

Default None

Mode Configuration mode

ip 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.

Syntax

```
[no] ip nat pool-group pool-group-name
[ha-group-id group-id]
```

Parameter	Description
pool-group-name	Name of the pool group.
ha-group-id *group-id*	HA group ID, 1-31.

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. See “Config Commands: Global” on page 79.)

Parameter	Description
member *pool-name*	Name of a configured IP address pool.

Default None

Mode Configuration mode

Usage For usage information, see “ip nat pool-group (for DNS64)” on page 515. The information in that section also applies here.

glid (for NAT64 override)

Description Configure a GLID to specify a NAT64 override action.

Note: This command applies only for configuring NAT64 override actions. To configure the LID for regular NAT64, see “lsn-lid” on page 530.

Syntax

```
[no] glid num
```

Parameter	Description
num	Specifies the GLID number, 1-1023.

This command changes the CLI to the configuration level for the specified GLID, where the following command is available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description

[no] dns64 {
disable |
prefix *ipv6-addr/nn* |
exclusive-answer
}
	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.
	prefix *ipv6-addr/nn* – Uses a different NAT64 prefix to synthesize IPv6 addresses in the reply to the client. You can use this option to load balance NAT64 service across multiple AX devices.
	exclusive-answer – Drops AAAA replies that contain specific IPv6 addresses or prefixes. In this case, the AX 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.

Default None

Mode Configuration mode

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)" on page 529 or "slb template policy" on page 537.

Syntax

```
[no] lsn-lid num
```

Parameter	Description
num	Specifies the LID number, 1-31.

This command changes the CLI to the configuration level for the specified LID, where the following command is available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
[no] **source-nat-pool** *pool-name*	Binds an IPv4 NAT pool to the LID.
[no] **user-quota-prefix-length** *mask-length*	Assign a user quota to all users of a specific IPv6 prefix.

Default None

Mode Configuration mode

nat64 alg

Description Enable or disable Application Level Gateway (ALG) support.

Syntax

```
[no] nat64 alg {ftp [options] | rtsp | sip | tftp}
{disable | enable}
```

Parameter	Description
ftp [*options*]	Enables or disables NAT64 ALG support for File Transfer Protocol (FTP). The options enable or disable command translation for compatibility with old FTP servers. NAT64 FTP ALG supports the following command translations:

		trans-eprt-to-port – EPRT (RFC 2428) to PORT
		trans-epsv-to-pasv – EPSV (RFC 2428) to PASV
		trans-lprt-to-port – LPRT (RFC 1639) to PORT
		trans-lpsv-to-pasv – LPSV (RFC 1639) to PASV
	rtsp	Enables or disables NAT64 ALG support for Real Time Streaming Protocol (RTSP).
	sip	Enables or disables NAT64 ALG support for Session Initiation Protocol (SIP).
	tftp	Enables or disables NAT64 ALG support for Trivial File Transfer Protocol (TFTP).
	disable | enable	Specifies whether to disable or enable ALG support.

Default ALG support for FTP is enabled by default, and all the command translation options are enabled by default. ALG support for RTSP, SIP, and TFTP is disabled by default.

Mode Configuration mode

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

```
nat64 fragmentation df-bit-transparency
{disable | enable}
```

Default Insertion of headers that have the more-fragments bit set to zero and the fragmentation-offset set to zero is disabled by default.

Mode Configuration mode

Usage This option applies to the IPv4-to-IPv6 traffic direction. When this option is enabled, headers are inserted when the IPv4 Don’t Fragment bit is ***not*** set.

nat64 fragmentation inbound

Description Configure fragmentation support for inbound packets.

Syntax

```
[no] nat64 fragmentation inbound
{
df-set send-icmp |
[df-set] drop |
[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] ipv6`	Enables fragmentation support for inbound IPv6 packets. The **df-set** option disallows override of the Don’t Fragment bit.

Default The following options are enabled by default:

- **ipv6**
- **df-set send-icmp**

Mode Configuration mode

nat64 fragmentation outbound

Description Configure fragmentation support for outbound packets.

Syntax

```
[no] 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

nat64 icmp

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

Syntax

```
[no] nat64 icmp
{send-on-port-unavailable |
send-on-user-quota-exceeded}
{
admin-filtered |
disable |
enable |
host-unreachable
}
```

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

host-unreachable	Sends code type 3, code 1 for IPv4, and type 1 code 3 for IPv6.

Default The default for **send-on-port-unavailable** is **disable**. The default for **send-on-user-quota-exceeded** is **admin-filtered**.

Mode Configuration mode

nat64 inside

Description Bind a class list to the NAT64 feature.

Syntax

```
[no] nat64 inside source class-list list-name
```

Default None

Mode Configuration mode

Usage To configure the class list, see "class-list (for NAT64)" on page 526.

nat64 prefix

Description See "nat64 prefix" on page 518.

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] nat64 tcp mss-clamp
{none | fixed n | subtract s [min n]}
```

Parameter	Description
none	Does not change the MSS value.
fixed *n*	Changes the MSS to the length you specify.
subtract *s* [**min** *n*]	Reduces the MSS if it is longer than the specified number of bytes. This option sets the MSS based on the following calculations:

– If MSS minus *S* is greater than *N*, subtract *S* from the MSS.

– If MSS minus *S* is less than or equal to *N*, set the MSS to *N*.

The subtract method of MSS clamping is used by default, with the following values:

S = 20 bytes

N = 476 bytes

Using these values, the default MSS clamping calculations are as follows:

– If MSS minus 20 is greater than 476, subtract 20 from the MSS.

– If MSS minus 20 is less than or equal to 476, set the MSS to 476.

Default

The **subtract** option is used by default. See above.

Mode

Configuration mode

nat64 tcp reset-on-error

Description

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

Syntax

```
[no] nat64 tcp reset-on-error outbound
{enable | disable}
```

Default

Enabled

Mode

Configuration mode

nat64 user-quota-prefix-length

Description

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

Syntax

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

Parameter	Description
mask-length	Prefix length, 1-128.

Default

128

Mode Configuration mode

Introduced in Release 2.6.6-P4

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 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.

slb template policy

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

Syntax

```
[no] slb template policy template-name
```

This command changes the CLI to the configuration level for the specified class list, where the following commands are available.

Note: The other configuration commands at this level are not applicable to DNS64 / NAT64.

Command	Description
`[no] class-list client-ip {l3-dest	l7-header [L7-header-name]}`	Extract the client's IP address from the Layer 7 header. **`l3-dest`** – Use the destination IP as the client's IP address. **`l7-header`** `[`*`L7-header-name`*`]` – Name of the Layer 7 header.
`[no] class-list name list-name`	Specifies the class list.

[no] class-list lid *num*

Configure a LID within the class list. This command changes the CLI to the configuration level for the LID, where the following command is available.

```
[no] dns64
{
disable |
prefix ipv6-addr/nn |
exclusive-answer
}
```

This command specifies the override action for IPv6 addresses that match the class list.

disable – Does not perform DNS64 processing on the client's DNS request. The client's request is forwarded to the DNS server, and the reply is sent to client without modification.

prefix *ipv6-addr/nn* – Uses a different NAT64 prefix to synthesize IPv6 addresses in the reply to the client. You can use this option to load balance NAT64 service across multiple AX devices.

exclusive-answer – Drops AAAA replies that contain specific IPv6 addresses or prefixes. In this case, the AX 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.

Default None

Mode Configuration mode

DNS64 / NAT64 Show Commands

This section describes the show commands for NAT64 / DNS64.

show dns64 statistics

Description Show statistics or DNS64.

Syntax **`show dns64 statistics`**

Mode Privileged EXEC and all configuration levels

Usage The following command shows DNS64 statistics:

```
AX#show 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
```

Table 14 describes the fields in the command’s output.

TABLE 14 show dns64 statistics fields

Field	Description
Query	Number of queries received from clients.
Response	Number of responses received from the DNS server. **Note:** The AX 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 AX 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 AX 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.

TABLE 14 show dns64 statistics fields (Continued)

Field	Description
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.
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 nat64 alg

Description Show Application Level Gateway (ALG) information for NAT64.

Syntax

```
show nat64 alg {ftp | rtsp | sip | tftp} config
```

Parameter	Description
ftp	Shows whether NAT64 ALG support for File Transfer Protocol (TFTP) 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:

```
AX#show nat64 alg rtsp config
NAT64 RTSP ALG is disabled on TCP port 554
```

show nat64 conversion

Description

Show the IPv4 version of an IPv6 address or the IPv6 version of an IPv4 address.

Syntax

```
show nat64 conversion
{ipv4-addr | ipv6-addr}
prefix NAT64-prefix
```

Parameter	Description
ipv4-addr | *ipv6-addr*	Specifies the IP address to convert. *ipv4-addr* – To display the IPv6 version of an IPv4 address, enter the IPv4 address. *ipv6-addr* – To display the IPv4 version of an IPv6 address, enter the IPv4 address.
prefix *NAT64-prefix*	Specifies the NAT64 prefix to use for the conversion.

Mode

All

Example

The following command shows the IPv4 version of IPv6 address 64:ff9b::c0a8:10a, using the well-known NAT64 prefix (64:ff9b::/96):

```
AX#show 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 nat64 full-cone-sessions

Description

Show currently active NAT64 full-cone sessions.

Syntax

```
show nat64 full-cone-sessions
[brief]
[pool pool-name]
```

Parameter	Description
brief	Displays only session statistics.
pool *pool-name*	Displays only the full-cone sessions that use a public IP address from the specified NAT pool.

Mode All

Table 15 describes the fields in this command's output.

TABLE 15 show nat64 full-cone-sessions fields

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	NAT pool from which the public IP address was assigned.
CPU	AX CPU on which the session resides.
Age	Number of seconds the session has been in effect.
Statistics (brief option)	
NAT64 TCP Full-cone Session Created	Number of TCP full-cone sessions created.
NAT64 TCP Full-cone Session Freed	Number of TCP full-cone sessions freed.
NAT64 UDP Full-cone Session Created	Number of UDP full-cone sessions created.
NAT64 UDP Full-cone Session Freed	Number of UDP full-cone sessions freed.
NAT64 Full-cone Session Creation Failed	Number of times an attempt to create a NAT64 full-cone session failed.

show nat64 inside-user

Description Show session information for a specific NAT64 inside client.

Syntax

```
show nat64 inside-user ipv6addr
```

Parameter	Description
ipv6addr	Specifies the inside IPv6 address of the user.

Mode All

Example The following command shows session information for NAT64 user 2001:10::100:

```
AX#show nat64 inside-user 2001:10::100
NAT64 User-Quota Sessions:
Inside IPv6                            NAT Address         ICMP   UDP    TCP    Pool            LID
--------------------------------------------------------------------------------------------------
-------
2001:10::100                            172.7.7.30          0      2      2      lsn0            1
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
```

Table 16 describes the fields in the command’s output.

TABLE 16 show nat64 inside-user fields

Field	Description
NAT64 User-Quota Sessions	Lists the following user-quota session information for the user: • Inside IPv6 – IPv6 address of the client • NAT Address – Client IPv4 NAT address from the LSN pool on the AX 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 AX device • Conns – Number of connections currently using the session • Pool – LSN NAT pool from which the NAT address for the session was selected • CPU – AX CPU on which the session resides • Age – Number of seconds the session has been in effect

TABLE 16 show nat64 inside-user fields (Continued)

Field	Description
NAT64 Data Sessions	Lists the following data session information for the user: • Prot – Protocol of the session • IP Type – Role of the IP address in the session: • Fwd Src – IPv6 address and protocol port of the client • Fwd Dst – Synthetic IPv6 address and 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 AX 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 nat64 prefixes

Description Show the IPv6 prefixes configured for NAT64.

Syntax

```
show nat64 prefixes
```

Mode All

Introduced in Release 2.6.6-P4

show nat64 statistics

Description Show statistics for NAT64.

Syntax

```
show nat64 statistics
```

Mode All

Table 17 describes the fields in this command’s output.

TABLE 17 show nat64 statistics fields

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.
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.

TABLE 17 show nat64 statistics fields (Continued)

Field	Description
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.
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-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.
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.

TABLE 17 show nat64 statistics fields (Continued)

Field	Description
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.
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 NAT-ted.
No Class-List Match	Number of times traffic did not match the LSN class list.

show nat64 user-quota-sessions

Description

Show NAT64 user-quota session information.

Syntax

```
show nat64 user-quota-sessions
[brief]
[pool pool-name]
[prefix ipv6addr/prefix-length]
[top num {all | icmp | tcp | udp}]
```

Parameter	Description
brief	Displays only statistics.

pool *pool-name* — Displays session information only for the specified NAT pool.

prefix *ipv6addr/ prefix-length* — Displays session information only for the specified IPv6 address(es).

top *num type* — Limits the display to the sessions with the highest counters for the specified resource type. You can specify 1-100.

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

Table 18 describes the fields in the command's output.

TABLE 18 show nat64 user-quota-sessions fields

Field	Description
Information for Individual Sessions:	
Inside IPv6	Inside IP address of the client.
Prefix NAT Address	Public IP address assigned to the client.
ICMP	Number of ICMP sessions from the quota that are in use.
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 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.
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.

TABLE 18 show nat64 user-quota-sessions fields (Continued)

Field	Description
NAT64 User-Quota Creation Failed	Number of times creation of a port mapping was unsuccessful because the user quota had no free mappings.
NAT64 TCP User-Quota Exceeded	Number of times the TCP quota for a user was exceeded.
NAT64 UDP User-Quota Exceeded	Number of times the UDP quota for a user was exceeded.
NAT64 ICMP User-Quota Exceeded	Number of times the ICMP quota for a user was exceeded.
NAT64 Extended 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.

Config Commands: DS-Lite

The commands in this chapter configure global settings for Dual-Stack Lite (DS-Lite). DS-Lite enables the AX device to act as an end-point for IPv4 traffic tunneled through an IPv6 link.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

DS-Lite Configuration Commands

This section describes the DS-Lite configuration commands.

class-list (for DS-Lite)

Description Configure an IP class list for use with Dual-Stack Lite (DS-Lite).

Syntax

```
[no] class-list {list-name | filename file}
```

Parameter	Description
list-name	Adds the list to the running-config.
filename **file**	Saves the list to a file.

This command changes the CLI to the configuration level for the specified class list, where the following commands are available.

Note: The other configuration commands at this level are not applicable to DS-Lite.

Command	Description
`[no] ipv6-addr/prefix-length lsn-lid num`	Adds an entry to the class list. *ipv6-addr/prefix-length* – Specifies the range of client IPv6 addresses on which to match. These are the IPv6 addresses of the customer DS-Lite routers. **lsn-lid** *num* – Specifies the LID number.

Default None

Mode Configuration mode

Usage Configure the DS-Lite LIDs before configuring the class-list entries. To configure an LID for DS-Lite, see "lsn-lid" on page 147.

As an alternative to configuring class entries on the AX device, you can configure the class list using a text editor on another device, then import the class list onto the AX device. To import a class list, see "import" on page 69.

For more information about DS-Lite, see the "Dual-Stack Lite" chapter in the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.

ds-lite alg

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

Syntax

```
[no] ds-lite alg
{ftp | pptp | rtsp | sip | tftp}
{enable | disable}
```

Parameter	Description
`ftp	pptp	rtsp	sip	tftp`	Specifies the protocol for which to disable or enable ALG support: **ftp** – File Transfer Protocol **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

ds-lite fragmentation inbound

Description Configure fragmentation support for inbound packets.

Syntax

```
[no] 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

ds-lite fragmentation outbound

Description Configure fragmentation support for outbound packets.

Syntax

```
[no] 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 overriding the Don’t Fragment bit.
`[df-set] drop`	Drops outbound fragmented packets. The **df-set** option disallows override of the Don’t Fragment bit.
`[df-set] ipv4`	Enables fragmentation support for outbound IPv4 packets. The **df-set** option disallows override of the Don’t Fragment bit.
`[df-set] send-icmpv6`	Enables sending of ICMPv6 unreachable messages for outbound IPv6 fragmented packets, and disallows overriding the Don’t Fragment bit. The **df-set** option disallows override of the Don’t Fragment bit.

Default By default, fragmentation for IPv6 tunnel packets is enabled but fragmentation of IPv4 packets within the tunnel is disabled. Override of the Don’t Fragment bit is enabled.

Mode Configuration mode

ds-lite icmp

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

Syntax

```
[no] ds-lite icmp
{send-on-port-unavailable |
send-on-user-quota-exceeded}
{
admin-filtered |
disable |
enable |
host-unreachable
}
```

Parameter	Description
send-on-port-unavailable	Sends ICMP Destination Unreachable message when there are no protocol ports available for NAT mappings.
send-on-user-quota-exceeded	Sends ICMP Destination Unreachable message when a a user quota is exceeded.
admin-filtered	Sends code type 3, code 13, administratively filtered.
disable	Disable ICMP Unreachable messages for the specified event.
enable	Enables ICMP Unreachable messages for the specified event.
host-unreachable	Sends code type 3, code 1 for IPv4, and type 1 code 3 for IPv6.

Default The default for **send-on-port-unavailable** is **disable**. The default for **send-on-user-quota-exceeded** is **admin-filtered**.

Mode Configuration mode

ds-lite inside source

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

Syntax

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

Parameter	Description
list-name	Specifies the class list.

Default None

Mode Configuration mode

ip-checksum-error

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

Syntax

```
[no] 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 AX device always drops other IPv4 traffic that has an invalid checksum.

Introduced in Release 2.6.6-P4

l4-checksum-error

Description

Configure handling of Layer 4 checksum errors in DS-Lite tunneled IP traffic.

Syntax

```
[no] ds-lite l4-checksum-error
{fix | drop | propagate}
```

Default

propagate

Mode

Configuration mode

Introduced in Release

2.6.6-P4

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 AX device always drops other IPv4 traffic that has an invalid checksum.

ds-lite port-reservation

Description

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

Syntax

```
[no] ds-lite port-reservation inside
ipv6-tunnel-source ipv6-tunnel-destination
ipv4-inside-addr inside-start-port
inside-end-port
nat nat-ipaddr nat-start-portnum nat-end-portnum
```

Parameter	Description
ipv6-tunnel-source	Inside client’s tunnel source IPv6 address.
ipv6-tunnel-destination	Inside client’s tunnel destination IPv6 address.
ipv4-inside-addr	Client IPv4 address.
inside-start-portnum	Beginning Layer 4 protocol port number in the port range to be mapped.
inside-end-port	Ending Layer 4 protocol port number in the port range to to be mapped.

nat *nat-ipaddr*	Public IPv4 address to map to the client IPv4 address.
nat-start-portnum	Beginning Layer 4 protocol port number to map to the inside port range.
nat-end-portnum	Ending Layer 4 protocol port number to map to the inside port range.

Default None

Mode Configuration mode

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

Parameter	Description
none	Does not change the MSS value.
fixed *n*	Changes the MSS to the length you specify.
subtract *s* [**min** *n*]	Reduces the MSS if it is longer than the specified number of bytes. This option sets the MSS based on the following calculations: – If MSS minus *S* is greater than *N*, subtract *S* from the MSS. – If MSS minus *S* is less than or equal to *N*, set the MSS to *N*. The subtract method of MSS clamping is used by default, with the following values: *S* = 40 bytes *N* = 416 bytes

Using these values, the default MSS clamping calculations are as follows:

– If MSS minus 40 is greater than 416, subtract 40 from the MSS.

– If MSS minus 40 is less than or equal to 416, set the MSS to 416.

Default The **subtract** option is used by default. See above.

Mode Configuration mode

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] ds-lite tcp reset-on-error outbound
{enable | disable}
```

Default Enabled

Mode Configuration mode

DS-Lite Show Commands

This section describes the show commands for DS-Lite.

show ds-lite alg

Description Show the current Application Level Gateway (ALG) configuration for DS-Lite.

Syntax

```
show ds-lite alg
{ftp | pptp | rtsp | sip | tftp} config
```

Mode All

show ds-lite full-cone-sessions

Description Shows currently active full-cone sessions.

Syntax

```
show ds-lite full-cone-sessions [pool pool-name]
```

Parameter	Description
pool *pool-name*	Shows sessions only for the specified pool. If you omit this option, sessions for all pools are shown.

Mode All

Table 19 describes the fields in this command's output.

TABLE 19 show ds-lite full-cone-sessions fields

Field	Description
Information for Individual Sessions:	
Prot	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 AX device for communicating with the IPv4 server.
Conns	Number of connections.
Pool	IP address pool from which the NAT address was assigned.
CPU	AX CPU on which the session resides.
Age	Number of seconds the session has been in effect.
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 ds-lite inside-user

Description

Show session information for a specific DS-Lite inside client.

Syntax

show ds-lite inside-user *ipv6addr*

Parameter	Description
ipv6addr	Specifies the inside IPv6 address of the user.

Mode

All

Example

The following command shows session information for DS-Lite user 2001:10::100:

```
AX#show ds-lite inside-user 2001:10::100
DS-Lite User-Quota Sessions:
Inside IPv6                            NAT Address         ICMP   UDP    TCP    Pool            LID
--------------------------------------------------------------------------------------------------
-------
2001:10::100                            172.7.7.30          0      2      2      lsn0            1
Total User-Quota Sessions Shown: 1

DS-Lite Full Cone Sessions:
Prot Inside IPv6                                     Inside Address         NAT Address
Conns  Pool             CPU Age
--------------------------------------------------------------------------------------------------
---------------------------------------
TCP  2001:10::100                               10.10.10.100:26504    172.7.7.30:27656      0
lsn0             2   120
UDP  2001:10::100                               10.10.10.100:48968    172.7.7.30:52232      1
lsn0             4    -
UDP  2001:10::100                               10.10.10.100:51775    172.7.7.30:29759      1
lsn0             4    -
TCP  2001:10::100                               10.10.10.100:26505    172.7.7.30:35849      1
lsn0             1    -
Total Full Cone Sessions: 4

DS-Lite Data Sessions:
Prot IP Type  IP Address and Port                                              Age  Hash Flags
----------------------------------------------------------------------------------------------
Tcp  Fwd Src  [2001:10::100]10.10.10.100:26505                                 0    1    NS
     Fwd Dst  [2001:10::1]172.7.7.100:80
     Rev Src  172.7.7.100:80
     Rev Dst  172.7.7.30:35849
Udp  Fwd Src  [2001:10::100]10.10.10.100:51775                                 300  4    NS
     Fwd Dst  [2001:10::1]172.7.7.100:5300
     Rev Src  172.7.7.100:5300
     Rev Dst  172.7.7.30:29759
Udp  Fwd Src  [2001:10::100]10.10.10.100:48968                                 300  4    NS
     Fwd Dst  [2001:10::1]172.7.7.100:5300
     Rev Src  172.7.7.100:5300
     Rev Dst  172.7.7.30:52232
```

Table 20 describes the fields in the command’s output.

TABLE 20 show ds-lite inside-user fields

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 AX 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
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 AX device • Conns – Number of connections currently using the session • Pool – LSN NAT pool from which the NAT address for the session was selected • CPU – AX CPU on which the session resides • Age – Number of seconds the session has been in effect

TABLE 20 show ds-lite inside-user fields (Continued)

Field	Description
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 AX device, 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 AX 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 ds-lite port-reservations

Description Show Layer 4 port reservations.

Syntax

```
show ds-lite port-reservations
```

Mode All

Table 21 describes the fields in this command’s output.

TABLE 21 show ds-lite port-reservations fields

Field	Description
Tunnel Src IPv6 Address	Source IPv6 address of the tunnel on which the AX device receives the client traffic.
Tunnel Dst IPv6 Address	Destination IPv6 address of the tunnel on which the AX device receives the client traffic.
Inside Address	Client IPv4 address.
Start	Beginning Layer 4 protocol port number in the port range to be mapped.
End	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.

TABLE 21 show ds-lite port-reservations fields (Continued)

Field	Description
Start	Beginning Layer 4 protocol port number to map to the inside port range.
End	Ending Layer 4 protocol port number to map to the inside port range.

show ds-lite statistics

Description Show global statistics related to DS-Lite.

Syntax

```
show ds-lite statistics
```

Mode All

Table 22 describes the fields in this command’s output.

TABLE 22 show ds-lite statistics fields

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.

TABLE 22 show ds-lite statistics fields (Continued)

Field	Description
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.
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.)

TABLE 22   show ds-lite statistics fields (Continued)

Field	Description
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.
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.
UDP Port Overloading Session Freed	Number of times a session created on an overloaded UDP port was freed.
Truncated Packet	Number of tunneled packets that were truncated because they were longer than the Maximum Transmission Unit (MTU) on the AX 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 NAT-ted.
No Class-List Match	Number of times traffic did not match the LSN class list.

TABLE 22 show ds-lite statistics fields (Continued)

Field	Description
Permit Class-List Drop	Number of packets dropped because they did not match the class list's permit list.

show ds-lite user-quota-sessions

Description Show currently active user quota sessions.

Syntax

```
show ds-lite user-quota-sessions
[brief]
[pool pool-name]
[top num {all | icmp | tcp | udp}]
```

Parameter	Description
brief	Displays only session statistics.
pool *pool-name*	Shows currently active full-cone sessions only for the specified pool. If you omit this option, sessions for all pools are shown.
top *num type*	Limits the display to the sessions with the highest counters for the specified resource type. You can specify 1-100. The resource type can be one of the following: **all** – Displays the sessions with the highest counters for all resource types (ICMP, TCP, and UDP). **icmp** – Displays the sessions with the highest counters for ICMP. **tcp** – Displays the sessions with the highest counters for TCP. **udp** – Displays the sessions with the highest counters for UDP.

Mode All

Table 22 describes the fields in this command's output.

TABLE 23 show ds-lite user-quota-sessions fields

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 Address	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 are in use.
TCP	Number of TCP 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.

Config Commands: Lightweight 4over6

The commands in this chapter configure global settings for the Lightweight 4over6 version of Dual-Stack Lite (DS-Lite).

Lightweight 4over6 enables the AX 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 AX device.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup log” on page 48 and “backup system” on page 50.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Lightweight 4over6 Configuration Commands

This section describes the global configuration commands for Lightweight 4over6. Also see “lw-406” on page 229.

lw-4o6 binding-table

Description Configure a binding table for Lightweight 4over6.

Syntax `[no] lw-4o6 binding-table name`

Parameter	Description
name	Name of the binding table.

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 Lightweight 4over6.

Command	Description
[**no**] *ipv6-tunnel-addr* [*ipv4-nat-addr* **port** *portnum* [**to** *portnum*]]	Creates a binding table for Lightweight 4over6. You can enter all the parameters below on the same command line. Alternatively, you can enter just the IPv6 tunnel address. In this case, the CLI changes to the configuration level for the individual binding entry, where you can specify the other parameters. *ipv6-tunnel-addr* – IPv6 address of the client CPE. This is the address of the remote end of the IPv6 tunnel between the AX device and the client CPE. *ipv4-nat-addr* – NAT address of the client. This is the IPv6 public address assigned to the client by the client’s CPE. This must be a host address, not a subnet address. **port** *portnum* [**to** *portnum*]– Protocol port number or range the CPE may use the as the

	source port in the IPv4 NAT address assigned to the client by the CPE.

Default None

Introduced in Release 2.6.6-P6

Mode Configuration mode

Usage The binding table does not take effect until you activate it. To activate a binding table, see "lw-4o6 use-binding-table" on page 574.

lw-4o6 ha-group-id

Description Assign the active Lightweight 4over6 bindings to an HA group. When you configure this option, active sessions that use bindings in the active Lightweight 4over6 binding table are synchronized to the standby AX device.

Syntax

```
[no] lw-4o6 ha-group-id group-id
```

Parameter	Description
group-id	HA group ID, 1-31.

Default None

Introduced in Release 2.6.6-P6

Mode Configuration mode

lw-4o6 hairpinning

Description Configure hairpinning for Lightweight 4over6 clients.

Syntax

```
[no] 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**

Introduced in Release 2.6.6-P6

Mode Configuration mode

lw-4o6 icmp-inbound

Description Configure handling of inbound IPv4 ICMP traffic for Lightweight 4over6 traffic. This applies to IPv4 traffic from the Internet fro sessions using Lightweight 4over6 bindings.

Syntax

```
[no] lw-4o6 icmp-inbound {drop | handle}
```

Parameter	Description
`drop`	Drops inbound ICMP traffic.
`handle`	Handles inbound ICMP traffic.

Default **handle**

Introduced in Release 2.6.6-P6

Mode Configuration mode

Usage The feature applies only to inbound IPv4 traffic that is received on the Lightweight 4over6 inside NAT interface. (See “lw-406” on page 229.)

lw-4o6 no-forward-match

Description

Enable ICMPv6 Destination Unreachable messages (type 1, code 5) from the AX device to the client CPE.

Syntax

```
[no] lw-4o6 no-forward-match send-icmpv6
```

Default

Disabled

Introduced in Release

2.6.6-P6

Mode

Configuration mode

Usage

The feature applies only to outbound traffic on the Lightweight 4over6 outside NAT interface. (See “lw-406” on page 229.)

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

lw-4o6 no-reverse-match

Description

Enable ICMP Destination Unreachable messages (type 3, code 1) from the AX device to IPv4 servers.

Syntax

```
[no] lw-4o6 no-reverse-match send-icmp
```

Default

Disabled

Introduced in Release

2.6.6-P6

Mode

Configuration mode

Usage

The feature applies only to inbound IPv4 traffic that is received on the Lightweight 4over6 inside NAT interface. (See “lw-406” on page 229.)

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 AX 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.

lw-4o6 use-binding-table

Description Activate a Lightweight 4over6 binding table.

Syntax

```
[no] lw-4o6 binding-table name
```

Parameter	Description
name	Name of the binding table.

Default Disabled

Introduced in Release 2.6.6-P6

Mode Configuration mode

Lightweight 4over6 Show Commands

This section describes the show commands for Lightweight 4over6.

show lw-4o6 binding-table

Description Show binding-table information for Lightweight 4over6.

Syntax

```
show lw-4o6 binding-table
[
files |
statistics |
tunnel-address ipv6addr [statistics]
]
```

Parameter	Description
files	Lists the Lightweight 4over6 binding tables on the AX device, and their status.
statistics	Displays binding-table statistics.

tunnel-address *ipv6addr* [**statistics**]	Displays information for the specified Lightweight 4over6 tunnel address. If you use the **statistics** option, statistics are listed.

Introduced in Release 2.6.6-P6

Mode All

show lw-4o6 statistics

Description Show statistics for Lightweight 4over6.

Syntax

```
show lw-4o6 statistics
```

Introduced in Release 2.6.6-P6

Mode All

Table 24 describes the fields in this command’s output.

TABLE 24 show lw-4o6 statistics fields

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).

TABLE 24 show lw-4o6 statistics fields (Continued)

Field	Description
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 binding-table entry. • The destination IP address matches the IPv4 NAT address of any binding-table entry. • Any self-hairpinning drops occur. (See above.)
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 AX 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. See “lw-4o6 no-forward-match” on page 573.
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. See “lw-4o6 no-reverse-match” on page 573.
Inbound ICMP Drops	Number of inbound IPv4 ICMP packets that were dropped. **Note:** This counter is incremented only if the feature is enabled. See “lw-4o6 icmp-inbound” on page 572.
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.
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.

Config Commands: Stateless NAT46

The commands in this chapter configure stateless NAT46. Stateless NAT46 enables IPv4 clients to reach IPv6 servers, without the need to maintain per-connection information on the AX device.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Stateless NAT46 Configuration Commands

This section describes the configuration commands for stateless NAT46.

nat46-stateless fragmentation inbound

Description

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

Syntax

```
[no] nat46-stateless fragmentation inbound
{ipv4 | drop | send-icmpv6}
```

Parameter	Description
ipv4	IPv4 fragmentation is allowed.
drop	IPv4 fragmentation is not allowed. Oversize packets are dropped. No ICMPv6 error message is sent.
send-icmpv6	IPv4 fragmentation is not allowed. Oversize packets are dropped, and an ICMPv6 error message is sent.

Default

send-icmpv6

Mode

Configuration mode

nat46-stateless fragmentation outbound

Description

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

Syntax

```
[no] nat46-stateless fragmentation outbound
{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

ipv6

Mode Configuration mode

nat46-stateless fragmentation outbound df-set

Description Change fragmentation support for IPv4 packets that have the Don’t Fragment bit set.

Syntax

```
[no] 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

nat46-stateless prefix

Description Configure a IPv6 prefix for stateless NAT46.

Syntax

```
[no] nat46-stateless prefix ipv6-prefix
```

Parameter	Description
ipv6-prefix	The 96-bit prefix used as the higher-order bits of the client’s IPv6 address.

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 AX 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.

nat46-stateless static-dest-mapping

Description

Configure static IPv4-IPv6 mappings for the IPv6 servers.

Syntax

```
[no] nat46-stateless static-dest-mapping
ipv4addr ipv6addr
[count num]
[ha-group-id num]
```

Parameter	Description
ipv4addr	IPv4 server address to which IPv4 clients will send requests.
ipv6addr	Server's IPv6 address. Specify the lowest address in the range.
count *num*	Specifies how many mappings to create. The IPv4 and IPv6 addresses of each mapping are incremented by 1 over the previous mapping.
ha-group-id *num*	Assigns the mappings to a High Availability (HA) group. You can specify 1-31.

Default

None

Mode

Configuration mode

Usage

You can configure a range of up to 1024 static mappings. You need to specify only the first mapping in the range, and how many mappings to create. The AX device then automatically creates additional mappings, up to the quantity you specify.

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 AX 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**

Stateless NAT46 Show Commands

This section describes the show commands for stateless NAT46.

show nat46-stateless statistics

Description Show stateless NAT46 statistics.

Syntax **show nat46-stateless statistics**

Mode All

Example The following command displays statistics for stateless NAT46:

```
AX(config)#show 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
```

Table 25 describes the fields in the command output.

TABLE 25 show nat46-stateless statistics fields

Field	Description
Outbound IPv4 packets received	Number of client IPv4 packets received by the AX device.
Outbound IPv4 packets dropped	Number of client IPv4 packets dropped by the AX device.
Outbound IPv4 fragment packets received	Number of IPv4 packet fragments received from clients by the AX device.
Outbound IPv6 destination unreachable	Number of times the IPv6 destination was unreachable.
Outbound IPv6 packets fragmented	Number of outbound IPv6 packets fragmented.
Inbound IPv6 packets received	Number of inbound IPv6 packets received.
Inbound IPv6 packets dropped	Number of inbound IPv6 packets dropped.
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.

TABLE 25 show nat46-stateless statistics fields (Continued)

Field	Description
HA is standby	Number of times the HA group the stateless NAT46 mappings are in was in the Standby state on this AX device.
Other errors	Number of errors other than those counted above.

Config Commands: 6rd

The commands in this chapter configure IPv6 rapid deployment (6rd). 6rd enables IPv6 clients to communicate with IPv6 servers over a service provider’s IPv4 network.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See “backup system” on page 50 and “backup log” on page 48.
- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

6rd Configuration Commands

This section describes the 6rd configuration commands.

6rd domain

Description

Configure 6rd domain settings.

Syntax

```
[no] 6rd domain domain-name
```

Parameter	Description
domain-name	String to describe the 6rd domain.

This command changes the CLI to the configuration level for the specified 6rd domain, where the following commands are available.

Note: The other configuration commands at this level are not applicable to 6rd.

Command	Description
[**no**] **br-ipv4-address** *ipv4addr* **ipv6-prefix** *ipv6addr/prefix-length*	Specifies the 6rd IPv4 address of the AX 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 AX 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 AX device. In this case, the High Availability (HA) state is applicable. Packets are forwarded only on the active AX device in the HA pair.

Note: The current release does not support use of an anycast address for 6rd.

[**no**] **ce-ipv4-network** *ipv4addr* {*subnet-mask* | */mask-length*}	Specifies the client IPv4 network, and the portion of the client's 6rd customer edge (CE) router IPv4 address that is common to all of the 6rd domain's clients. For example, if your deployment uses 10.0.0.0/8 for all CE router IPv4 addresses in the 6rd domain, specify the following: **ce-ipv4-network 10.0.0.0 /8**
[**no**] **mtu** *bytes*	Specifies the maximum transmission unit (MTU) for the IPv6 tunnel. You can specify 1280-1480 bytes.

Default

There are no 6rd domains configured by default. When you create one, it has the following default settings:

- **br-ipv4-address** and **ipv6-prefix** – Not set
- **ce-ipv4-network** – Not set
- **mtu** – 1480

Mode

Configuration mode

Example

For the AX BR address, you can use either an IP address configured on an AX interface or a High Availability (HA) floating-IP address. If you use an IP address configured on an AX interface, the 6rd domain is not synchronized to the standby AX 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. To configure an IPv4 address on an AX data interface, see "ip address" on page 210. To configure an HA floating-IP address, see "floating-ip" on page 125.

6rd fragmentation inbound

Description

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

Syntax

```
[no] 6rd 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.

6rd fragmentation outbound

Description Configure fragmentation support for oversize outbound IPv6 packets. These are packets from the AX device, forwarded on behalf of 6rd clients to IPv6 servers.

Syntax

```
[no] 6rd fragmentation outbound
{
drop |
ipv6 |
send-icmp |
send-icmpv6
}
```

Note: For information about the **df-set** option, see "6rd fragmentation outbound df-set" on page 589.

Parameter	Description
`drop`	Drops oversize packets without sending an ICMPv6 error message to the client. Fragmentation is not 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

6rd fragmentation outbound df-set

Description Configure the AX response to oversize outbound IPv6 packets that have the Don’t Fragment bit set.

Syntax

```
[no] 6rd 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

6rd Show Commands

This section describes the show commands for 6rd.

show 6rd statistics

Description Show 6rd statistics.

Syntax

```
show 6rd statistics [domain-name]
```

Mode All

Example

The following command displays statistics for the 6rd domain “6rd1”:

```
AX(config-6rd)#show 6rd 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
```

Table 26 describes the fields in this command’s output.

TABLE 26 show 6rd statistics fields

Field	Description
Outbound TCP packets received	Number of client-to-server TCP packets received from clients.
Outbound UDP packets received	Number of client-to-server UDP packets received from clients.
Outbound ICMP packets received	Number of client-to-server ICMP packets received from clients.
Outbound other packets received	Number of fragmented client-to-server packets received from clients.
Outbound packets dropped	Number of client-to-server packets dropped by the AX device because they were larger than the MTU of the outgoing interface.

TABLE 26 show 6rd statistics fields (Continued)

Field	Description
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 AX 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 AX device because they were larger than the MTU of the outgoing interface.
Inbound IPv4 destination unreachable	Number of server-to-client packets that could not reach the destination of the IPv4 tunnel.
Inbound Fragmented IPv4	Number server-to-client packets fragmented into multiple IPv4 packets.
Inbound Fragmented IPv6 in tunnel	Number server-to-client packets fragmented into multiple IPv6 packets before being sent in the IPv4 tunnel.
Unknown 6rd delegated prefix	Number of packets received that had an unknown 6rd delegated prefix.
Packet too big	Number of packets received by the AX device from clients or servers that were larger than the MTU of the AX 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 AX device was in the standby state, so the IP address could not be used.
Fragment processing errors	Number of times the AX 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.

Config Commands: Logging Template

This chapter describes the commands for configuring logging templates. Logging templates are applicable to IPv6 migration features.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

ip nat template logging

Description

Configure a template for external logging of LSN / DS-Lite 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 command is available.

(The other commands are common to all CLI configuration levels. See “Config Commands: Global” on page 79.)

Parameter	Description
`[no] batched-logging-disable`	Disables batching of multiple log messages in the same external logging packet. When this option is enabled, only a single log message is placed in each packet.

[no] facility *facility-name*

Specifies the logging facility to use. For a list of available facilities, enter the following command: **facility ?**

[no] format *option*

Reduces the size of external traffic logs. You can enable one of the following data reduction options:

binary – Uses a unique A10 Binary Logging format to represent the log messages.

compact – Uses ASCII text format. It reduces the log size by using operational codes (“opcodes”) for event and protocol names, and by using hexadecimal representation for IPv4 addresses and port numbers.

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.

For more information about these logging formats, see the “NAT Logging” chapter of the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.

[no] include-destination

Includes the destination IP addresses and protocol ports in NAT port mapping logs.

[no] include-http [l4-session-info | method]

Includes additional information into the log messages.

l4-session-info – Includes TCP session information.

method – Includes the HTTP method; for example: GET or POST.

[no] include-radius-attribute {imei | imsi | msisdn} {http-requests | port-mappings | sessions}

Includes the client mobile number in Carrier Grade NAT (CGN) traffic logs. The AX 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:

imei – International Mobile Equipment Identity

imsi – International Mobile Subscriber Identity

msisdn – Mobile Station International ISDN Number[*]

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.

[no] log *option*

Enables logging for specific options:

fixed-nat {http-requests {host | url} | port-mappings {both | creation} | sessions} – Enables logging for Fixed-NAT.

- **http-requests [host | url]** – Enables logging of information from HTTP requests.
- **port-mappings** – Logs Fixed-NAT port mappings. The **both** option logs Fixed-NAT

[*] More than one explanation of the acronym “MSISDN” can be found online. For simplicity, this document uses only one of them to define the acronym, then uses the acronym thereafter.

session creation and deletion. The **creation** option logs Fixed-NAT session creation only.

sessions – Logs Fixed-NAT session creation and deletion.

fixed-nat-user-ports – Enables logging of all Fixed-NAT ports assigned to clients.

http-requests {host | url} – Enables logging of information from HTTP requests.

host – Logs the hostname requested by the client.

url – Logs the URL requested by the client.

port-mappings {both | creation} – Enables logging of LSN port mapping events.

both – Logs mapping creation and mapping deletion.

creation – Logs mapping creation only.

port-overloading – Logs all port overloading sessions.

sessions – Enables logging of data session events.

[no] log-receiver radius secret *secret-string*

Enables use of RADIUS for external logging. The *secret-string* is the password required by the RADIUS server for authentication requests.

Note: The "**no**" form of the command returns the logging method to its default, Syslog.

[no] resolution

Specifies the precision of the timestamps in log messages.

seconds – Log message timestamps are precise to within one whole second.

10-milliseconds – Log message timestamps are precise to within 1/100 second (10 milliseconds).

[no] **rfc-custom header use-alternate-timestamp**

Use the following timestamp format:

YYYY MMM DD HH:*MM*:*SS*

Enabling this option disables use of timestamps formatted in compliance with RFC 5424, The Syslog Protocol.

[no] **rfc-custom message** *feature type string*

Customizes log message strings for external logging.

The *feature* can be one of the following:

- **6rd-nat64** – Message strings for 6rd-NAT64 traffic.
- **ds-lite** – Message strings for DS-Lite traffic.
- **http-request-got** – Message strings for HTTP request logs. The *message-string* must be in the following format: “MSG-ID [STRUCTURED-DATA] MSG”
- **lsn** – Message strings for CGN traffic.
- **nat64** – Message strings for NAT64 traffic.
- **session-created** – Message strings for session creation.
- **session-deleted** – Message strings for session deletion.

The *type* can be one of the following:

- **port-allocated**
- **port-freed**
- **port-batch-allocated**
- **port-batch-freed**
- **fixed-nat-allocated**
- **fixed-nat-freed**

Note: The **fixed-nat-allocated** and **fixed-nat-freed** message *types* apply only to *feature* types **lsn** and **nat64**.

The *string* specifies the fields and text to use in the message strings. (For *string* syntax information, see the “RFC 5424 Header Support For External Logging” section in the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.)

`[no]` **`rule http-requests`** *`option`*

Configures rules for HTTP request logging. You can set the following options:

`dest-port` *`portnum`* – 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

`log-every-http-request` – Logs every HTTP request in a client session. Without this option, only the first request in the session is logged.

`max-url-len` *`max-number-of-characters`* – Maximum number of characters logged for each URL string. You can specify 100-1000 characters.

Note: Some limitations may apply. See “Usage” below.

`[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`

`4 | warning`

`5 | notification`

```
6 | information
7 | debugging
```

`[no] source-port {portnum | any}` Specifies the source protocol port the AX device uses to send out log messages to the external log servers.
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 AX device randomly selects a source-port for each logging packet.

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 the AX device through Smart NAT.

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.
- **facility** – local0
- **format** – default
- **include-destination** – disabled
- **include-http** – 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. (See the *AX Series 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-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.

- To set the template as the default LSN / DS-Lite logging template, see "ip nat lsn logging default-template" on page 465.
- To assign the template to an LSN / DS-Lite pool, see "ip nat lsn logging pool" on page 466.

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 Table 27:

TABLE 27 Maximum URL Characters Logged

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.

Example

The following commands configure external logging for LSN / DS-Lite traffic events, using the same template for all LSN / DS-Lite pools:

```
AX5200(config)#slb server syslog1 192.168.1.100
AX5200(config-real server)#port 514 udp
AX5200(config-real server)#exit
```

```
AX5200(config)#slb service-group syslog udp
AX5200(config-slb svc group)#member syslog1:514
AX5200(config-slb svc group)#exit
AX5200(config)#ip nat template logging lsn_logging
AX5200(config-nat logging)#log port-mappings
AX5200(config-nat logging)#service-group syslog
AX5200(config-nat logging)#exit
AX5200(config)#ip nat lsn logging default-template lsn_logging
```

slb server

Description Configure a server for external logging.

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

Parameter	Description
server-name	Server name, 1-31 characters.
ipaddr	IP address of the server in either IPv4 or IPv6 format. The address is required only if you are creating a new server.

This command changes the CLI to the configuration level for the specified service-group, where the following command is available:

Command	Description
[**no**] **health-check** [*monitor-name*]	Enables health monitoring of the server. The *monitor-name* specifies the name of a configured health monitor. If you omit this command or you enter it without the *monitor-name* option, the default Layer 3 (ICMP) health monitor is used.
[**no**] **port** *port-num* {**tcp** | **udp**}	Specifies the TCP or UDP port on which the server listens for log traffic. **disable** | **enable** – Disables or re-enables the port. [**no**] **health-check** [*monitor-name*] [**follow-port** *port-num*]– Enables health monitoring for a server.. The *monitor-*

name option specifies the name of a configured health monitor.

The **follow-port** *port-num* option specifies another real port upon which to base this port's health status. Both the real port and the port to use for the real port's health status must be the same type, TCP or UDP. By default, this option is not set.

If you omit the **health-check** command or you enter it without the *monitor-name* option, the default UDP health monitor is used. (See below.)

`stats-data-disable | stats-data-enable` – Disables or enables statistical data collection for the port.

Default There is no default logging server configuration. For health monitoring defaults, see below.

Mode Configuration mode

Usage The normal form of the **slb 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. The AX Series supports both address formats.

Default Health Monitoring

The following health monitors are enabled by default.

- ICMP – Server health check. Every 5 seconds, the AX 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 AX device. If the server does not reply after the fourth attempt (the first attempt followed by 3 retries), the AX device sets the server state to DOWN.
- TCP – Every 5 seconds, the AX 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 AX device by sending a TCP SYN ACK. If the port does not reply after the fourth attempt, the AX device sets the port state to DOWN.
- UDP – Protocol port health check. Every 5 seconds, the AX 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.

slb service-group

Description

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

Syntax

```
[no] slb service-group group-name udp
```

Parameter	Description
group-name	Name of the group, 1-31 characters.

This command changes the CLI to the configuration level for the specified service-group, where the following command is available:

Note: The other configuration commands at this level are not applicable to logging.

Command	Description
[no] member *server-name*:*portnum* **[disable | enable] [priority** *num*] **[stats-data-disable | stats-data-enable]**	Adds the external log server and UDP port to the service group. *server-name*:*portnum* – Server name, and protocol port number on the server. **disable | enable** – Disables or re-enables the server and port, for this service group only. **priority** *num* – Sets the preference for this server and port, 1-16. **stats-data-disable** – Disables statistical data collection for the service-group member.

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.

Show Commands

This section lists the show commands related to logging template configuration.

show ip nat logging keywords

Description Show valid keywords for RFC 5424 custom messages.

Syntax

```
show ip nat logging keywords feature event
```

Option	Description
feature	Specifies the feature, which can be one of the following: **6rd-nat64** – Message strings for 6rd-NAT64 traffic. **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. **session-deleted** – Message strings for session deletion.
event	Specifies the *event* type, which can be one of the following (depending on the *feature*): **port-allocated** **port-freed** **port-batch-allocated** **port-batch-freed** **fixed-nat-allocated** **fixed-nat-freed**

Mode All

Introduced in Release 2.6.6-P4

show ip nat logging statistics

Description

Show statistics for external logging.

Syntax

```
show ip nat logging statistics
```

Mode

All

show ip nat logging tcp-svr-status

Description

Displays status information for the TCP connections to logging servers.

Syntax

show ip nat logging tcp-svr-status template *template-name*

Option	Description
template-name	Specifies the name of the active logging template. (This is the template set as the default CGN logging template.)

Mode

All

Introduced in Release

2.6.6-P4

Example

The following command displays the status of the AX device's TCP connections to syslog servers:

```
AX#show ip nat 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
```

Table 28 describes the fields in the command output.

TABLE 28 show ip nat logging tcp-svr-status template

Field	Description
Server	Name of the syslog server.

TABLE 28 show ip nat logging tcp-svr-status template (Continued)

Field	Description
No. of TCP connections	Status of the TCP connections to the server. The status is shown as follows: `Established-Connections / Data-CPUs` To optimize performance, the AX device establishes a separate TCP session from each data CPU to each syslog server. The *Established-Connections* value is the number of connections that currently are established. The *Data-CPUs* value is the number of data CPUs on the AX device. This number varies depending on the AX model.
Status	Connection status: • OK – All AX TCP connections to the syslog server are functioning normally. • Retrying – Some connections are not up, and the AX device is sending SYNs to try to establish the missing connections.

show ip nat template logging

Description Displays the configuration of a logging template.

Syntax

```
show ip nat template logging template-name
```

Mode All

show slb server

Description Show information about real servers.

Syntax

```
show slb server
[[server-name [port-num] detail] config]
```

Option	Description
server-name [[*port-num*] **detail**]	Shows information only for the specified server or port. If you omit this option, information is shown for all real servers and ports. The **detail** option shows statistics for the specified server or port. This option also displays the

	name of the server or port template bound to the server or port.
config	Shows the SLB configuration of the real servers.

Mode All

show slb service-group

Description Show SLB service-group information.

Syntax

```
show slb service-group [group-name] [config]
```

Option	Description
group-name	Shows information only for the specified service group. If you omit this option, information is shown for all service groups configured on the AX Series device.
config	Shows the SLB configuration of the service groups.

Mode All

Config Commands: Fixed-NAT

This chapter describes the commands for Fixed-NAT.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

Note: For Fixed-NAT, use of a NAT64 prefix with mapping to a class list is not supported.

Fixed-NAT Configuration Command

This section describes the configuration command for Fixed-NAT.

fixed-nat

Description Configure Fixed-NAT.

Syntax

```
[no] fixed-nat
inside
  {start-ipaddr [netmask {/nn | ipaddr}]
  end-addr netmask {/nn | ipaddr} |
  ip-list list-name}
nat
  {start-ipaddr [netmask {/nn | ipaddr}]
  end-addr netmask {/nn | ipaddr} |
  ip-list list-name}
[dynamic-pool-size num]
[ha-group-id group-num]
```

```
[ports-per-user num]
[session-quota quota-num]
[usable-nat-ports starting-port ending-port]
```

Parameter	Description
inside *options*	IP address range(s) of inside clients. To specify a single range: *starting-inside-address* – Beginning (lowest-numbered) inside client address. *ending-inside-address* – Ending (highest-numbered) inside client address. **netmask** *mask* – Network mask, in the applicable format: IPv4 – */mask-length* IPv6 – *mask-length* To specify multiple ranges: **ip-list** *list-name* – Name of a configured IP list. (See “ip-list” on page 132.)
nat *options*	Range(s) of NAT addresses. To specify a single range: *starting-nat-address* – Beginning (lowest-numbered) NAT address. (For syntax information, see *starting-inside-address* above.) *ending-nat-address* – Ending (highest-numbered) NAT address. (For syntax information, see *starting-inside-address* above.) To specify multiple ranges: **ip-list** *list-name* – Name of a configured IP list. (See “ip-list” on page 132.)
dynamic-pool-size *num*	Number of protocol ports on each NAT address to set aside for use by clients who run out of their reserved ports.
ha-group-id *group-num*	HA group ID.

ports-per-user *num*	Number of protocol ports to allocate to each new client. You can specify 1-64512.
session-quota *quota-num*	Maximum number of sessions that can be created for a given client. You can specify 1-2147483647.
usable-nat-ports *starting-port ending-port*	Range of protocol ports that can be allocated to clients. You can specify 1024-65535.

Default Not set

Mode Configuration mode

Usage See the *AX Series IPv4-to-IPv6 Transition Solutions Guide*.

Fixed-NAT Show Commands

This section describes the show commands for Fixed-NAT.

show fixed-nat alg

Description Show Application Level Gateway (ALG) statistics for Fixed-NAT.

Syntax

```
show fixed-nat alg
{ftp | pptp | rtsp | sip | tftp}
statistics
```

Parameter	Description
ftp | pptp | rtsp | sip | tftp	Specifies the protocol: **ftp** – File Transfer Protocol (FTP) **pptp** – Point-to-Point Tunneling Protocol (PPTP) Generic Routing Encapsulation (GRE) **rtsp** – Real Time Streaming Protocol (RTSP) **sip** – Session Initiation Protocol (SIP) **tftp** – Trivial File Transfer Protocol (TFTP)

Mode

All

Example

For examples, see “show ip nat lsn alg” on page 485.

show fixed-nat full-cone-sessions

Description

Show Fixed-NAT full-cone sessions.

Syntax

```
show fixed-nat full-cone-sessions
[
ds-lite [nat-address ipaddr] |
nat-address ipaddr |
nat44 [nat-address ipaddr] |
nat64 [nat-address ipaddr]
]
```

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.

Mode

All

show fixed-nat inside-user

Description

Show Fixed-NAT information for a specific inside client.

Syntax

```
show fixed-nat inside-user {ipv4addr | ipv6addr}
{port-mapping | quota-used}
```

Parameter	Description
`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 fixed-nat nat-address

Description Display Fixed-NAT address information.

Syntax

```
show fixed-nat nat-address ipv4addr
[
portnum [tcp | udp | icmp] |
port-mapping
]
```

Parameter	Description
portnum [**tcp** | **udp** | **icmp**]	Specifies the protocol port. The **tcp** | **udp** | **icmp** option specifies the protocol. If you omit this option, the output applies to TCP ports. In the case of Fixed NAT, if you use the simplified syntax in this section, the same port ranges are used for each protocol. The TCP port range assigned to a Fixed NAT client is always the same as the UDP and ICMP port ranges assigned to that client.
port-mapping	Displays Fixed-NAT port mappings for a specific NAT address.

Mode All

show fixed-nat statistics

Description Show statistics for Fixed-NAT.

Syntax

```
show fixed-nat statistics
```

Mode All

Table 29 describes the fields in this command’s output.

TABLE 29 show fixed-nat statistics fields

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.
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.
Sessions User Quota Exceeded	Number of times a client exceeded their data session quota.

TABLE 29 show fixed-nat statistics fields (Continued)

Field	Description
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 Full-Cone Created	Total number of NAT64 UDP full-cone sessions created that used ALG support.
NAT64 UDP ALG Full-Cone Freed	Total number of NAT64 UDP full-cone sessions freed that used ALG support.
Full-Cone Session Creation Failed	Number of times creation of a full-cone session failed.
NAT44 Endpoint-Independent Mapping Matched	Number of times the NAT44 mapping assigned to a client was reused for subsequent traffic for that client. (This is the benefit provided by Endpoint independent mapping.)
NAT64 Endpoint-Independent Mapping Matched	Number of times the NAT64 mapping assigned to a client was reused for subsequent traffic for that client.

TABLE 29 show fixed-nat statistics fields (Continued)

Field	Description
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.)
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.
NAT44 Endpoint-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.
NAT64 Endpoint-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.
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.
NAT44 Hairpin Session Created	Total number of NAT44 hairpin sessions created.
NAT64 Hairpin Session Created	Total number of NAT64 hairpin sessions created.
Fixed NAT LID not Enabled	Number of times Fixed-NAT could not be performed because the Fixed-NAT LID was disabled.
Fixed NAT LID Standby Drop	Number of packets dropped because the Fixed-NAT LID is in an HA group, and this AX 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.

Config Commands: Server Resource Commands

Configure server resources for external logging for IPv6 migration features.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

slb buff-thresh

Description Fine-tune thresholds for server buffer queues.

Caution: **Do not use this command except under advisement by A10 Networks.**

Syntax

```
[no] slb buff-thresh hw-buff num
relieve-thresh num sys-buff-low num
sys-buff-high num
```

Parameter	Description
hw-buff *num*	IO buffer threshold. For each CPU, if the number of queued entries in the IO buffer reaches this threshold, fast aging is enabled and no more IO buffer entries are allowed to be queued on the CPU’s IO buffer.
relieve-thresh *num*	Threshold at which fast aging is disabled, to allow IO buffer entries to be queued again.

sys-buff-low *num*	Threshold of queued system buffer entries at which the AX begins refusing new incoming connections.
sys-buff-high *num*	Threshold of queued system buffer entries at which the AX device drops a connection whenever a packet is received for that connection.

Mode Configuration mode

slb fast-path-disable

Description Disable fast-path packet inspection.

Syntax

```
[no] slb fast-path-disable
```

Default Fast processing of packets is enabled by default.

Mode Configuration mode

Usage Fast processing of packets maximizes performance by using all the underlying hardware assist facilities. Typically, the feature should remain enabled. The option to disable it is provided only for troubleshooting, in case it is suspected that the fast processing logic is causing an issue. If you disable fast-path processing, ACOS does not perform a deep inspection of every field within a packet.

slb gateway-health-check

Description Enable gateway health monitoring.

Syntax

```
slb gateway-health-check
[interval seconds [timeout seconds]]
```

Parameter	Description
interval *seconds*	Specifies the amount of time between health check attempts, 1-180 seconds.
timeout *seconds*	Specifies how long the AX device waits for a reply to any of the ARP requests, 1-60 seconds.

Default The default interval is 5 seconds. The default timeout is 15 seconds.

Mode

Configuration mode

Usage

Gateway health monitoring uses ARP to test the availability of nexthop gateways. When the AX device needs to send a packet through a gateway, the AX device begins sending ARP requests to the gateway.

- If the gateway replies to any ARP request within a configurable timeout, the AX device forwards the packet to the gateway.
- The ARP requests are sent at a configurable interval. The AX device waits for a configurable timeout for a reply to any request. If the gateway does not respond to any request before the timeout expires, the AX device selects another gateway and begins the health monitoring process again.

slb l2l3-trunk-lb-disable

Description

Disable or re-enable trunk load balancing.

Syntax

```
[no] slb l2l3-trunk-lb-disable
```

Default

Enabled

Mode

Configuration mode

Usage

When trunk load balancing is enabled, the AX device load balances outbound Layer 2/3 traffic among all the ports in a trunk. The round-robin method is used to load balance the traffic. For example, in a trunk containing ports 1-4, the first Layer 2/3 packet is sent on port 1. The second packet is sent on port 2. The third packet is sent on port 3, and so on.

If you disable trunk load balancing, the lead port was always used for outbound traffic. The other ports were standby ports in case the lead port went down.

Trunk load balancing applies only to Layer 2/3 traffic, and is enabled by default. However, the CLI provides a command to disable trunk load balancing, in case there is a need to do so. Disabling trunk load balancing causes the AX device to use only the lead port for outbound traffic.

slb msl-time

Description

Configure the maximum session life for client-server sessions. The maximum session life controls how long the AX device maintains a session table entry for a client-server session after the session ends.

Syntax

```
[no] slb msl-time seconds
```

Parameter	Description
seconds	Number of seconds a client session can remain in the session table following completion of the session. You can specify 1-40 seconds.

Default

2 seconds

Mode

Configuration mode

Usage

The maximum session life allows time for retransmissions from clients or servers, which can occur if there is an error in a transmission. If a retransmission occurs while the AX device still has a session entry for the session, the AX device is able to forward the retransmission. However, if the session table entry has already aged out, the AX device drops the retransmission instead.

The maximum session life begins aging out a session table entry when the session ends:

- TCP – The session ends when the AX device receives a TCP FIN from the client or server.
- UDP – The session ends after the AX device receives a server response to the client’s request. If the reply is fragmented, the maximum session life begins only after the last fragment is received.

Note: For UDP sessions, the maximum session life is used only if UDP aging is set to **short**, instead of **immediate**. UDP aging is set in the UDP template bound to the UDP virtual port. The default setting is **short**.

slb server

Description

Configure a server for DNS64 / NAT64 (“slb server” on page 518) or for external session logging (“slb server” on page 601).

slb service-group

Description Configure a service group for DNS64 / NAT64 ("slb service-group" on page 520) or for external session logging ("slb service-group" on page 603).

slb ssl-module

Description Disable the SSL acceleration module.

Syntax

```
[no] slb ssl-module software
```

Default SSL acceleration modules are enabled.

Mode Configuration mode

Usage This command applies only to add-on SSL acceleration modules, not to the on-board SSL processors.

slb template dns

Description Configure DNS settings.

Syntax

```
[no] slb template dns template-name
```

Parameter	Description
template-name	Name of the template, 1-31 characters.

This command changes the CLI to the configuration level for the specified DNS template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See "Config Commands: Global" on page 83.)

Command	Description
[no] class-list lid *num*	Configures a DNS caching rule. The settings in the rule apply to queries for the domain names mapped to this rule in the class list. [**no**] **conn-rate-limit** *rate* **per** *interval* – Specifies the maximum rate allowed for queries. If queries exceed the specified rate, the over-limit action is applied. You can specify 1-4294967295

DNS connections per 1-65535 100-millisecond (ms) intervals.

dns {**cache-enable** | **cache-disable**} – Specifies whether to cache replies to queries for the domain name.

[**no**] **dns ttl** *num* – Number of seconds the AX device caches DNS replies. You can specify 1-65535 seconds.

[**no**] **dns weight** *num* – Specifies the numeric value used when cache entries need to be removed to make room for new entries. You can assign a weight of 1-7. Lower-weighted objects are removed before higher weighted objects.

Cache more than 60% full, entries with weight 1 are eligible to be removed.

Cache more than 70% full, entries with weight 1 or 2 are eligible to be removed.

Cache more than 80% full, entries with weights 1-4 are eligible to be removed.

Cache more than 90% full, entries with weights 1-6 are eligible to be removed.

Note: A DNS reply begins aging as soon as it is cached and continues aging even if the cached reply is used after aging starts. Use of a cached reply does not reset the age of that reply.

[**no**] **over-limit-action** *action* – Specifies the action to take if the query rate exceeds the configured limit:

dns-cache-disable – Disables caching.

dns-cache-enable – Enables caching.

forward – Forwards the request to the DNS server.

lockout *minutes* – Stops accepting new requests for the specified number of minutes, 1-1023.

log – Generates a log message when the query rate is exceeded.

reset – Resets the connection with the client.

[no] class-list name *name*

Applies a class list to the template.

[no] default-policy [cache | nocache]

Specifies the default action to take when a query does not match any class-list entries.

[no] disable-cache

Disables DNS caching on all virtual DNS ports that use the template.

[no] dns-log-enable period *minutes*

Enables logging for DNS caching. The **period** option specifies how often log messages are generated. You can specify 1-10000 minutes.

[no] malformed-query {drop | forward *service-group-name***}**

Specifies the action to take for malformed DNS queries:

drop – Drops malformed queries.

forward – Sends the queries to the specified service group. With either option, the malformed queries are not sent to the DNS virtual port.

[no] max-cache-size *num*

Specifies the maximum number of entries that can be cached per VIP. The maximum configurable amount depends on the amount of RAM installed on the AX device. For details, contact A10 Networks.

Default

The configuration does not have a default DNS template. If you configure one, the template has the following default values:

- **class-list name** – not set
- **class-list lid** – Not set. When you configure an LID, it has the following default values:
  - **conn-rate-limit** – not set
  - **dns** {**cache-enable** | **cache-disable**} – **cache-disable**
  - **dns ttl** – Global DNS caching TTL value, which is 300 seconds by default. (See “slb dns-cache-age” on page 492.)
  - **dns weight** – 1
  - **over-limit-action** – **cache-enable**

- **default-policy** – **nocache**
- **disable-cache** – caching is enabled
- **dns-log-enable** – disabled
- **malformed-query** – **drop**
- **max-cache-size** – maximum allowed on the entire system

Mode

Configure

Usage

The normal form of this command creates a DNS template. The “**no**” form of this command removes the template.

You can bind only one DNS template to a virtual port. However, you can bind the same DNS template to multiple ports.

For DNS64, bind the template to virtual port type **dns-udp**. Virtual port type **dns** applies to DNS security (**malformed-query** option).

DNS templates are not supported with stateless load-balancing methods.

slb template policy

Description

Configure a template of Policy-Based SLB (PBSLB) settings.

Syntax

```
[no] slb template policy template-name
```

This command changes the CLI to the configuration level for the specified PBSLB template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See “Config Commands: Global” on page 83.)

Command	Description
`[no] class-list client-ip {l3-dest | l7-header [header-name]}`	Specifies the IP address to use for matching entries in an IP class list. **l3-dest** – Matches based on the destination IP address in packets from clients. **l7-header** [*header-name*] – Matches based on the IP address in the specified header in packets

from clients. The *header-name* specifies the name of the header to use. If you do not specify a header name, the X-Forwarded-For header is used.

`[no] class-list lid` *`num`*

Configures an IP limiting rule for the IP limiting feature. This command changes the CLI to the configuration level for the rule, where the following commands are available:

[**no**] **conn-limit** *num* – Specifies the maximum number of concurrent connections allowed for a client. You can specify 0-1048575. Connection limit 0 immediately locks down matching clients.

[**no**] **conn-rate-limit** *num* **per** *num-of-100ms* – Specifies the maximum number of new connections allowed for a client within the specified limit period. You can specify 1-4294967295 connections. The limit period can be 100-6553500 milliseconds (ms), specified in increments of 100 ms.

[**no**] **request-limit** *num* – Specifies the maximum number of concurrent Layer 7 requests allowed for a client. You can specify 1-1048575.

[**no**] **request-rate-limit** *num* **per** *num-of-100ms* – Specifies the maximum number of Layer 7 requests allowed for the client 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.

Note: The class-list **request-limit** and **request-rate-limit** options apply only to HTTP, fast-HTTP, and HTTPS virtual ports.

These options, when configured in a policy template, are applicable only in policy templates that are bound to virtual ports. These options are not applicable in policy templates bound to virtual servers (rather than individual ports), or in policy templates used for system-wide PBSLB.

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.

[**no**] **over-limit-action** [**forward** | **reset**] [**lockout** *minutes*] [**log** *minutes*] – Specifies the action to take when a client exceeds one or more of the limits. The command also configures lockout and enables logging. The action can be one of the following:

– drop – The AX device drops that traffic. If logging is enabled, the AX device also generates a log message. (There is no **drop** keyword. This is the default action.)

– **forward** – The AX device forwards the traffic. If logging is enabled, the AX device also generates a log message.

– **reset** – For TCP, the AX device sends a TCP RST to the client. If logging is enabled, the AX device also generates a log message.

The **lockout** option 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.

The **logging** option 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 AX 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).

`[no] class-list name name` Applies an IP class list to the template.

Default

The AX device does not have a default policy template. When you configure one, the template has the following default settings:

- **class-list client-ip** – Client’s IP address is used.
- **class-list name** – not set
- **class-list lid** – Not set. When you create one, the limiting rule has the following default values:
  - **conn-limit** – Not set
  - **conn-rate-limit** – Not set

- **request-limit** – Not set
- **request-rate-limit** – Not set
- **over-limit-action** – Drop. There is no default lockout period. Logging is disabled by default. The default logging period is 0 (no wait period).

Mode Configuration mode

Usage The normal form of this command creates a policy template. The “**no**” form of this command removes the template.

You can bind only one policy template to a virtual port. However, you can bind the same policy template to multiple ports.

slb template port

Description Configure a template of SLB settings for service ports on real servers.

Syntax

```
[no] slb template port template-name
```

Parameter	Description
template-name	Name of the template, 1-31 characters.

This command changes the CLI to the configuration level for the specified real port template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See “Config Commands: Global” on page 79.)

Command	Description
[no] **conn-limit** *max-connections* [**resume** *connections*] [**no-logging**]	Specifies the maximum number of connections allowed on ports that use this template. The *max-connections* option specifies the maximum number of concurrent connections, 0-8000000. The **resume** *connections* option specifies the maximum number of connections the port can have before the AX device resumes use of the port. You can specify 1-1048575 connections.

The **no-logging** option disables logging for the feature.

[no] conn-rate-limit *connections* **[per {100ms | 1sec}] [no-logging]**

Limits the rate of new connections the AX device is allowed to send to ports that use this template. When a real port reaches its connection limit, the AX device stop selecting the port to serve client requests.

connections – Maximum of new connections allowed on the port. You can specify 1-1048575 connections.

per {100ms | 1sec} – Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (**1sec**).

The **no-logging** option disables logging for the feature.

[no] dest-nat

Enables destination Network Address Translation (NAT) on ports that use this template.

Destination NAT is enabled by default, but is automatically disabled in Direct Server Return (DSR) configurations. You can re-enable destination NAT on individual ports for deployment of mixed DSR configurations, which use backup servers across Layer 3 (in different subnets).

[no] dscp *number*

Sets the differentiated services code point (DSCP) value in the IP header of a client request before sending the request to ports that use this template. The *number* specifies the DSCP value and can be 1-63. By default, DSCP is not set by the AX device.

[no] dynamic-member-priority *num* **decrement** *delta*

Configure service-group priority settings for ports on dynamically created servers. The *num* option sets the initial TTL for dynamically created service-group members, and can be 1-16.

The *delta* option specifies how much to decrement the TTL if the IP address is not included in the DNS reply, and can be 0-7. When configuring the service group, add the port template to the member.

[**no**] **health-check** [*monitor-name*]

Enables health monitoring of ports that use this template. The *monitor-name* specifies the name of a configured health monitor.

[**no**] **inband-health-check** [**retry** *maximum-retries*] [**reassign** *maximum-reassigns*]

Supplements the standard Layer 4 health checks by using client-server traffic to check the health of service ports.

retry *maximum-retries* – Each client-server session has its own retry counter. The AX device increments a session's retry counter each time a SYN ACK is late. If the retry counter exceeds the configured maximum number of retries allowed, the AX device sends the next SYN for the session to a different server. The AX device also resets the retry counter to 0. You can set the retry counter to 0-7 retries.

reassign *maximum-reassigns* – Each real port has its own reassign counter. Each time the retry counter for any session is exceeded, the AX device increments the reassign counter for the server port. If the reassign counter exceeds the configured maximum number of reassignments allowed, the AX device marks the port down.

In this case, the port remains down until the next time the port successfully passes a standard health check. Once the port passes a standard health check, the AX device starts using the port again and resets the reassign counter to 0. You can set the reassign counter to 0-255 reassignments. The default is 25 reassignments.

Note: A10 Networks recommends that you continue to use standard Layer 4 health monitoring even if you enable in-band health monitoring. Without standard health monitoring, a server port marked down by an in-band health check remains down.

[**no**] **slow-start** [**from** *starting-conn-limit*] [**times** *scale-factor* | **add** *conn-incr*] [**every** *interval*] [**till** *ending-conn-limit*]

Provides time for real ports that use the template to ramp-up after TCP/UDP service is enabled, by temporarily limiting the number of new connections on the ports.

from *starting-conn-limit* – Maximum number of concurrent connections to allow on the service port after it first comes up. You can specify from 1-4095 concurrent connections. The default is 128.

times *scale-factor* | **add** *conn-incr* – Amount by which to increase the maximum number of concurrent connections allowed. You can use one of the following methods to specify the increment:

> **times** *scale-factor* – The scale factor is the number by which to multiply the starting connection limit. For example, if the scale factor is 2 and the starting connection limit is 128, the AX device increases the connection limit to 256 after the first ramp-up interval. The scale factor can be 2-10. The default is 2.
>
> **add** *conn-incr* – As an alternative to specifying a scale factor, you can instead specify how many more concurrent connections to allow. You can specify 1-4095 new connections.

every *interval* – Number of seconds between each increase of the number of concurrent connections allowed. For example, if the ramp-up interval is 10 seconds, the number of concurrent connections to allow is increased every 10 seconds. The ramp-up interval can be 1-60 seconds. The default is 10 seconds.

till *ending-conn-limit* – Maximum number of concurrent connections to allow during the final ramp-up interval. After the final ramp-up interval, the slow start is over and does not limit further connections to the server. You can specify from 1-65535 connections. The default is 4096.

`Note:` If a normal runtime connection limit is also configured (for example, by the **conn-limit** command), and the normal connection limit is smaller than the slow-start ending connection limit, the AX device limits slow-start connections to the maximum allowed by the normal connection limit.

`source-nat` *`pool-name`* Specifies the IP NAT pool to use for assigning source IP addresses to client traffic sent to ports that use this template. When the AX device performs NAT for a port that is bound to the template, the device selects an IP address from the pool.

`[`**`no`**`]` **`weight`** *`number`* Specifies the load-balancing preference for ports that use this template. You can specify 1-100. A higher weight gives more favor to the server and port relative to the other servers and ports. Default is 1.

This option applies only to the **weighted-least-connection**, **service-weighted-least-connection**, and **weighted-rr** (weighted round robin) load-balancing methods.

Default The AX device has a default real port template, called “default”. The default port template has the same default settings as the individual parameters you can configure in the template. Here are the defaults:

- **conn-limit** – 8000000 (8 million)
- **conn-rate-limit** – Not set; when enabled, the default sampling rate is **per 1-sec**.
- **dest-nat** – Not set
- **dscp** – Not set
- **dynamic-member-priority** – priority 16 and delta 0

- **health-check** – If you omit this command or you enter it without the *monitor-name* option, the default TCP or UDP health monitor is used:
    - TCP – Every 30 seconds, the AX device sends a connection request (TCP SYN) to the specified TCP port on the server. The port passes the health check if the server replies to the AX device by sending a TCP SYN ACK.
    - UDP – Every 30 seconds, the AX 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.
- **inband-health-check** – Disabled. When enabled, the feature has the following defaults: *maximum-retries* – 2; *maximum-reassigns* – 25.
- **slow-start** – Not set
- **source-nat** – Not set
- **weight** – 1

Mode

Configuration mode

Usage

The normal form of this command creates a real port template. The “**no**” form of this command removes the template.

You can bind only one real port template to a real port. However, you can bind the real port template to multiple real ports.

Some of the parameters that can be set using a template can also be set or changed on the individual port.

- If a parameter is set (or changed from its default) in both a template and on the individual port, the setting on the individual port takes precedence.
- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual port, the setting in the template takes precedence.

If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

slb template server

Description

Configure server settings.

Syntax

```
[no] slb template server template-name
```

Parameter	Description
template-name	Name of the template, 1-31 characters.

This command changes the CLI to the configuration level for the specified real server template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See “Config Commands: Global” on page 79.)

Command	Description
`[no] conn-limit max-connections [resume connections] [no-logging]`	Specifies the maximum number of connections allowed on real servers that use this template. The *max-connections* option specifies the maximum number of concurrent connections, 0-8000000. The **resume** *connections* option specifies the maximum number of connections the server can have before the AX device resumes use of the server. You can specify 1-1048575 connections. The **no-logging** option disables logging for the feature.
`[no] conn-rate-limit connections [per {100ms	1sec}] [no-logging]`	Limits the rate of new connections the AX device is allowed to send to servers that use this template. When a real server reaches its connection limit, the AX device stops selecting the server for client requests.

connections – Maximum of new connections allowed on a server. You can specify 1-1048575 connections.

`per {100ms | 1sec}` – Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals.

The **no-logging** option disables logging for the feature.

`[no]` **`dns-query-interval`** *`minutes`*

Specifies how often the AX device sends DNS queries for the IP addresses of dynamic real servers. You can specify 1-1440 minutes (one day).

`[no]` **`dynamic-server-prefix`** *`string`*

Specifies the prefix added to the front of dynamically created servers. You can specify a string of 1-3 characters.

`[no]` **`health-check`** `[`*`monitor-name`*`]`

Enables health monitoring of ports that use this template. 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 ICMP health monitor is used: an ICMP ping (echo request) is sent every 30 seconds. If the ping fails 2 times consecutively, the AX device sets the server state to DOWN.

`[no]` **`max-dynamic-server`** *`num`*

Specifies the maximum number of dynamic real servers that can be created for a given hostname. You can specify 1-1023.

`[no]` **`min-ttl-ratio`** *`num`*

Specifies the minimum initial value for the TTL of dynamic real servers. The AX device multiplies this value by the DNS query interval to calculate the minimum TTL value to assign to the dynamically created server. The min-ttl-ratio can be 1-15.

[**no**] **slow-start** [**from** *starting-conn-limit*] [**times** *scale-factor* | **add** *conn-incr*] [**every** *interval*] [**till** *ending-conn-limit*]

Provides time for real ports that use the template to ramp-up after TCP/UDP service is enabled, by temporarily limiting the number of new connections on the ports.

from *starting-conn-limit* – Maximum number of concurrent connections to allow on the server after it first comes up. You can specify from 1-4095 concurrent connections. The default is 128.

times *scale-factor* | **add** *conn-incr* – Amount by which to increase the maximum number of concurrent connections allowed. You can use one of the following methods to specify the increment:

> **times** *scale-factor* – The scale factor is the number by which to multiply the starting connection limit. For example, if the scale factor is 2 and the starting connection limit is 128, the AX device increases the connection limit to 256 after the first ramp-up interval. The scale factor can be 2-10. The default is 2.
>
> **add** *conn-incr* – As an alternative to specifying a scale factor, you can instead specify how many more concurrent connections to allow. You can specify 1-4095 new connections.

every *interval* – Number of seconds between each increase of the number of concurrent connections allowed. For example, if the ramp-up interval is 10 seconds, the number of concurrent connections to allow is increased every 10 seconds. The ramp-up interval can be 1-60 seconds. The default is 10 seconds.

till *ending-conn-limit* – Maximum number of concurrent connections to allow during the final ramp-up interval. After the final ramp-up interval, the slow start is over and does not limit further connections to the server. You can specify from 1-65535 connections. The default is 4096.

`Note:` If a normal runtime connection limit is also configured on the server (for example, by the **conn-limit** command), and the normal connection limit is smaller than the slow-start ending connection limit, the AX device limits slow-start connections to the maximum allowed by the normal connection limit.

Default

The AX device has a default real server template, called “default”. The default server template has the same default settings as the individual parameters you can configure in the template. Here are the defaults:

- **conn-limit** – 8000000 (8 million)
- **conn-rate-limit** – Not set; when enabled, the default sampling rate is **per 1-sec**.
- **dns-query-interval** – 10 minutes
- **dynamic-server-prefix** – DRS (for “Dynamic Real Servers”)
- **health-check** – If you omit this command or you enter it without the *monitor-name* option, the default ICMP health monitor is used. An ICMP ping (echo request), sent every 30 seconds. If the ping fails 2 times consecutively, the AX device sets the server state to DOWN.
- **max-dynamic-server** – 255
- **min-ttl-ratio** – 2
- **slow-start** – Not set

Mode

Configuration mode

Usage

The normal form of this command creates a real server template. The “**no**” form of this command removes the template.

You can bind only one real server template to a real server. However, you can bind the real server template to multiple real servers.

Some of the parameters that can be set using a template can also be set or changed on the individual server.

- If a parameter is set (or changed from its default) in both a template and on the individual server, the setting on the individual server takes precedence.
- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual server, the setting in the template takes precedence.

If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

slb template virtual-port

Description

Configure a template of SLB settings for virtual service ports.

Syntax

```
[no] slb template virtual-port template-name
```

Parameter	Description
template-name	Name of the template, 1-31 characters.

This command changes the CLI to the configuration level for the specified virtual port template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See "Config Commands: Global" on page 79.)

Command	Description
`[no] aflow`	Enables aFlow control. aFlow helps avoid packet drops and retransmissions when a real server port reaches its configured connection limit. When aFlow is enabled, the AX device queues HTTP/HTTPS packets from clients when a server port reaches a configured connection limit, instead of dropping them. The AX device then monitors the port, and begins forwarding the queued packets when connections become available again. To prevent flooding of the port, the AX device forwards the queued packets at a steady rate.

aFlow applies only to HTTP and HTTPS virtual ports.

[**no**] **conn-limit** *max-connections* [**reset**] [**no-logging**]

Specifies the maximum number of connections allowed on virtual ports that use this template.

The *max-connections* option specifies the maximum number of concurrent connections, 0-8000000.

The **reset** option specifies the action to take for connections after the connection limit is reached on the virtual server port. By default, excess connections are dropped. If you change the action to reset, the connections are reset instead. Excess connections are dropped by default. The **no-logging** option disables logging for the feature.

[**no**] **conn-rate-limit** *connections* [**per** {**100ms** | **1sec**}] [**reset**] [**no-logging**]

Limits the rate of new connections the AX device is allowed to send to virtual service ports that use this template. When a virtual service port reaches its connection limit, the AX device stop selecting the port to serve client requests.

connections – Maximum of new connections allowed on the virtual service port. You can specify 1-1048575 connections.

per {100ms | 1sec} – Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (**1sec**).

reset – Send a reset (RST) to a client after the connection rate has been exceeded. By default (without this option), the AX device silently drops the request.

If you configure a limit for a virtual server and also for an individual virtual service port, the AX device uses the lower limit.

The **no-logging** option disables logging for the feature.

`[no] ignore-tcp-msl`

Immediately reuse TCP sockets after session termination, without waiting for the SLB Maximum Session Life (MSL) time to expire. This option is disabled by default.

`[no] reset-unknown-conn`

Enables sending of a TCP Reset (RST) in response to a session mismatch. A session mismatch occurs when the AX device receives a TCP packet for a TCP session that is not in the active session table on the AX device. (For more information, see the “TCP Reset Option for Session Mismatch” section in the “Server and Port Templates” chapter of the *AX Series Application Delivery and Server Load Balancing Guide*.)

Default

The AX device has a default virtual port template, called “default”. The default virtual port template has the same default settings as the individual parameters you can configure in the template. Here are the defaults:

- **aflow** – disabled
- **conn-limit** – 8000000 (8 million)
- **conn-rate-limit** – Not set; when enabled, the default sampling rate is **per 1-sec**.
- **ignore-tcp-msl** – disabled
- **reset-unknown-conn** – disabled

Mode

Configuration mode

Usage

The normal form of this command creates a virtual service port template. The “**no**” form of this command removes the template.

You can bind only one virtual service port template to a virtual service port. However, you can bind the virtual service port template to multiple virtual service ports.

Some of the parameters that can be set using a template can also be set or changed on the individual virtual port.

- If a parameter is set (or changed from its default) in both a template and on the individual virtual port, the setting on the individual virtual port takes precedence.
- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual virtual port, the setting in the template takes precedence.

If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

aFlow Operation

aFlow control is triggered when either of the following occurs:

- If connection limit is configured on the real server or real port – The backend real server or real port reaches its configured connection limit.
- If connection limit is not configured on the real server or real port – The response time of the backend real server or real port increases dramatically. The response time is the time between when the AX device forwards a request to the server, when the AX device receives the first reply packet from the server.

When aFlow control is triggered, the AX device queues request packets instead of forwarding them to the server. After the response time returns to normal, the AX device sends the queued packets to the server.

Note: In the current release, it is recommended to use the first method for triggering aFlow, by configuring connection limits on the real servers or real ports. The second method of triggering aFlow is still being refined and is considered to be in Beta status.

slb template virtual-server

Description Configure a template of SLB settings for virtual servers.

Syntax

```
[no] slb template virtual-server template-name
```

Parameter	Description
template-name	Name of the template, 1-31 characters.

This command changes the CLI to the configuration level for the specified virtual server template, where the following commands are available.

(The other commands are common to all CLI configuration levels. See "Config Commands: Global" on page 79.)

Command	Description
`[no] conn-limit` *`max-connections`* `[reset]` `[no-logging]`	Specifies the maximum number of connections allowed on virtual servers that use this template. The *max-connections* option specifies the maximum number of concurrent connections, 0-8000000. The **`reset`** option specifies the action to take for connections after the connection limit is reached on the virtual server. By default, excess connections are dropped. If you change the action to reset, the connections are reset instead. Excess connections are dropped by default. The **no-logging** option disables logging for the feature.
`[no] conn-rate-limit` *`connections`* `[per {100ms | 1sec}]` `[reset]` `[no-logging]`	Limits the rate of new connections the AX device is allowed to send to servers that use this template. When a real server reaches its connection limit, the AX device stop selecting the server for client requests. *connections* – Maximum of new connections allowed on a server. You can specify 1-1048575 connections. **`per {100ms	1sec}`** – Specifies whether the connection rate limit applies to one-second intervals or 100-ms intervals. The default is one-second intervals (**1sec**). **`reset`** – Send a reset (RST) to a client after the connection rate has been exceeded. By default

(without this option), the AX device silently drops the request.

If you configure a limit for a server and also for an individual port, the AX device uses the lower limit.

The **no-logging** option disables logging for the feature.

[**no**] **icmp-rate-limit** *normal-rate* **lockup** *max-rate* *lockup-time*

Configures ICMP rate limiting for the virtual server, to protect against denial-of-service (DoS) attacks.

normal-rate – Maximum number of ICMP packets allowed per second. If the virtual server receives more than the normal rate of ICMP packets, the excess packets are dropped until the next one-second interval begins. The normal rate can be 1-65535 packets per second.

lockup *max-rate* – Maximum number of ICMP packets allowed per second before the AX device locks up ICMP traffic to the virtual server. When ICMP traffic is locked up, all ICMP packets are dropped until the lockup expires. The maximum rate can be 1-65535 packets per second. The maximum rate must be larger than the normal rate.

lockup-time – Number of seconds for which the AX device drops all ICMP traffic to the virtual server, after the maximum rate is exceeded. The lockup time can be 1-16383 seconds.

[**no**] **subnet-gratuitous-arp**

Enable gratuitous ARPs for all VIPs in subnet VIPs. A subnet VIP is a range of VIPs created from a range of IP addresses within a subnet.

Note: This option applies only to VIPs that are created using a range of subnet IP addresses. The option has no effect on VIPs created with a single IP address.

Default

The AX device has a default virtual server template, called “default”. The default virtual server template has the same default settings as the individual parameters you can configure in the template. Here are the defaults:

- **conn-limit** – 8000000 (8 million)
- **conn-rate-limit** – Not set; when enabled, the default sampling rate is **per 1-sec**.
- **icmp-rate-limit** – Not set. If you enable it, specifying a maximum rate (lockup rate) and lockup time is optional. If you do not specify them, lockup does not occur.
- **subnet-gratuitous-arp** – Disabled. The AX device sends gratuitous ARPs for only the first IP address in a subnet VIP.

Mode

Configuration mode

Usage

The normal form of this command creates a virtual server template. The “**no**” form of this command removes the template.

You can bind only one virtual server template to a virtual server. However, you can bind the virtual server template to multiple virtual servers.

Some of the parameters that can be set using a template can also be set or changed on the individual virtual server.

- If a parameter is set (or changed from its default) in both a template and on the individual virtual server, the setting on the individual virtual server takes precedence.
- If a parameter is set (or changed from its default) in a template but is not set or changed from its default on the individual virtual server, the setting in the template takes precedence.

If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

slb virtual-server

Description

Configure settings for a virtual server. (Virtual servers are also called “virtual IP addresses” or “VIPs”).

Syntax

```
[no] slb virtual-server name {ipaddr | ipv6-addr}
```

This command creates the virtual server and changes the CLI to the configuration level for the virtual server. For information about the commands at this level, see “Config Commands: Virtual Servers” on page 645.

Config Commands: Virtual Servers

This chapter describes the commands for configuring virtual servers.

To access this configuration level, enter the **slb virtual-server** *vipaddr vip-name* command at the global Config level.

To display configured virtual servers, use the **show slb virtual-server** command.

Note: The commands in this chapter apply to virtual servers (also called "VIPs"), not to real servers. To configure real servers, see "slb server" on page 620.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See "clear" on page 59.
- **debug** – See "debug" on page 64.
- **do** – See "do" on page 117.
- **end** – See "end" on page 123.
- **exit** – See "exit" on page 124.
- **no** – See "no" on page 155.
- **show** – See "Show Commands" on page 689.
- **write** – See "write terminal" on page 78.

arp-disable

Description Disable ARP replies from a virtual server.

Syntax

```
[no] arp-disable
```

Default ARP replies are enabled by default.

Mode Virtual server

Usage Use this command if you do not want the AX Series device to reply to ARP requests to the virtual server's IP address. For example, you can use this command to put a VIP out of service on one AX device and use that device as a switch or router for another AX device providing SLB for the VIP.

When you disable ARP replies for a VIP, redistribution of routes to the VIP is automatically disabled.

Example The following command disables ARP replies:

```
AX(config-slb virtual server)#arp-disable
```

disable

Description Disable a virtual server.

Syntax `[no] disable [when-all-ports-down]`

Parameter	Description
`when-all-ports-down`	Automatically disables the virtual server if all its service ports are down. If OSPF redistribution of the VIP is enabled, the AX device also withdraws the route to the VIP in addition to disabling the virtual server.

Default Virtual servers are enabled by default. The **when-all-ports-down** option is disabled by default.

Mode Virtual server

Example The following commands disable virtual server “vs1”:

```
AX(config)#slb virtual-server vs1
AX(config-slb virtual server)#disable
```

enable

Description Enable a virtual server.

Syntax `[no] enable`

Default Enabled

Mode Virtual server

Example The following commands re-enable virtual server “vs1”:

```
AX(config)#slb virtual-server vs1
AX(config-slb virtual server)#enable
```

extended-stats

Description Enable collection of peak connection statistics for a virtual server.

Syntax `[no] extended-stats`

Default Disabled

Mode Virtual server

ha-dynamic

Description Enable VIP-based failover.

Syntax `[no] ha-dynamic server-weight`

Parameter	Description
server-weight	Amount to subtract from the HA group’s priority value for each real server that becomes unavailable. The weight can be 1-255.

Default Not set

Mode Virtual server

Example The following commands assign virtual server VIP2 to HA group 6 and enable VIP-based failover for the virtual server.

```
AX(config)#slb virtual VIP2 192.168.10.22
AX(config-slb virtual server)#ha group 6
AX(config-slb virtual server)#ha-dynamic 10
```

ha-group

Description Add a virtual server to a High-Availability (HA) group.

Syntax `[no] ha-group group-id`

Default None.

Mode Virtual server

Example The following commands assign virtual server “vs1” to HA group 1:

```
AX(config)#slb virtual-server vs1
AX(config-slb virtual server)#ha-group 1
```

port

Description Configure a virtual port on a virtual server, for the DNS proxy used for DNS64.

Syntax

```
[no] port port-number dns-udp
```

Default N/A

Mode Virtual server

Usage The normal form of this command creates a new or edits an existing virtual port. The CLI changes to the configuration level for the virtual port. (See “Config Commands: Virtual Server Ports” on page 651.)

The “**no**” form of this command removes the specified virtual port from current virtual server.

redistribution-flagged

Description Flag this VIP to selectively enable or disable redistribution of it by OSPF.

Syntax

```
[no] redistribution-flagged
```

Default Not set. The VIP is automatically redistributed if VIP redistribution is enabled in OSPF.

Mode Virtual server

Usage Use this option if you want to redistribute only some of the VIPs rather than all of them.

Selective VIP redistribution also requires configuration in OSPF. See the description of the **vip** option in “redistribute” on page 321.

stats-data-disable

Description Disable collection of statistical data for the virtual server.

Syntax

```
stats-data-disable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual server

stats-data-enable

Description Enable collection of statistical data for the virtual server.

Syntax

```
stats-data-enable
```

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual server

Usage To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally. (See “stats-data-enable” on page 184.)

template logging

Description Bind a logging template to the virtual server.

Syntax

```
[no] template logging template-name
```

Default None

Mode Virtual server

template policy

Description Bind a policy template to the virtual server.

Syntax

```
[no] template policy template-name
```

Default None

Mode Virtual server

template virtual-server

Description

Bind a virtual server template to the virtual server.

Syntax

```
[no] template virtual-server template-name
```

Default

The virtual server template named “default” is bound to virtual servers by default. The parameter settings in the default virtual server template are automatically applied to the new virtual server, unless you bind a different virtual server template to the virtual server.

Mode

Virtual server

Usage

If a parameter is set individually on this virtual server and also is set in a virtual server template bound to this virtual server, the individual setting on this virtual server is used instead of the setting in the template.

To configure a virtual server template, see “slb template virtual-server” on page 640.

Example

The following commands configure a virtual server template called “vs-tmplt1” that sets ICMP rate limiting, and bind the template to a virtual server:

```
AX(config)#slb template server vs-tmplt1
AX(config-vserver)#icmp-rate-limit 25000 lock 30000 60
AX(config-vserver)#exit
AX(config)#slb virtual-server vip1 10.10.10.2
AX(config-slb virtual server)#template virtual-server vs-tmplt1
```

Config Commands: Virtual Server Ports

This chapter describes the commands for configuring virtual ports.

To access this configuration level, enter the **port** *port-num port-type* command at the configuration level for a virtual server.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

access-list

Description

Apply an Access Control List (ACL) to a virtual server port.

Syntax

```
[no] access-list {acl-num | name acl-name}
     [source-nat-pool
       {pool-name | pool-group-name}
         [sequence-number num]]
```

Parameter	Description
acl-num | **name** *acl-name*	Number of a configured IPv4 ACL (*acl-num*), or the name of a configured IPv6 ACL (**name** *acl-name*).

`source-nat-pool` *`pool-name`* `|` *`pool-group-name`* `[`**`sequence-number`** *`num`*`]`

Name of a configured IP source NAT pool or pool group. Use this option if you are configuring policy-based source NAT. Source NAT is required if the real servers are in a different subnet than the VIP.

The **sequence-number** *num* option specifies the position of this ACL in the sequence of ACLs that are associated with IP source NAT pools and which are assigned to this virtual port. The sequence number is important because the AX device will use the IP addresses in the pool associated with the first ACL that matches the traffic.

By default, the ACL sequence is based on the order in which you apply them to the virtual port. The first ACL has sequence number 1, the second ACL has sequence number 2, and so on. You can specify 1-32 as the sequence number. To view the sequence, use the **show running-config** command to view the configuration for this virtual port.

Default

N/A

Mode

Virtual port

Usage

The ACL must be configured before you can apply it to a virtual port. To configure an ACL, see “access-list (standard)” on page 80 and “access-list (extended)” on page 82.

To permit or deny traffic on the virtual port, specify an ACL but do not specify a NAT pool.

To configure policy-based source NAT, specify an ACL *and* a NAT pool. Use an extended ACL. The source IP address must match on the client address. The destination IP address must match on the real server address. The action must be permit. The NAT pool is used only for traffic that matches the ACL. This configuration allows the virtual port to have multiple pools, and to select a pool based on the traffic.

Example

The following commands configure a standard ACL to deny traffic from subnet 10.10.10.x, and apply the ACL to the inbound traffic direction on virtual port 8080 on virtual server “slb1”:

```
AX(config)#access-list 99 deny 10.10.10.0 0.0.0.255
AX(config)#slb server slb1
AX(config-slb virtual server)#port 8080 http
AX(config-slb virtual server-slb virtua...)#access-list 99
```

Example The following commands configure policy-based source NAT, by binding ACLs to NAT pools on the virtual port.

```
AX(config)#slb virtual-server vs1 10.10.10.100
AX(config-slb virtual server)#port 80 tcp
AX(config-slb virtual server-slb virtua...)#access-list 30 source-nat-pool
pool1
AX(config-slb virtual server-slb virtua...)#access-list 50 source-nat-pool
pool2
```

conn-limit

Description Set the connection limit for a virtual port.

Syntax

```
[no] conn-limit number [reset] [no-logging]
```

Parameter	Description
number	Connection limit, 0-8000000 (8 million); 0 means no limit.
reset	Sends a connection reset to the client, if the connection limit has been reached. If you omit this option, the connection is silently dropped and no reset is sent to the client.
no-logging	Disables logging for this feature.

Default Not set. If you set a limit, the default action for any new connection request after the limit has been reached is to silently drop the connection, without sending a reset to the client. Logging is enabled by default.

Mode Virtual port

Usage The normal form of this command changes the current port’s connection limit.

The “**no**” form of this command resets the port’s connection limit to its default value.

The connection limit puts a hard limit on the number of concurrent connections supported by the port. No more connections will be put on the port if its number of current connections is already equal to or bigger than the limit.

If you change the connection limiting configuration on a virtual port or virtual server that has active sessions, or in a virtual-port or virtual-server template bound to the virtual server or virtual port, the current connection counter for the virtual port or server in show command output and in the GUI may become incorrect. To avoid this, do not change the connection limiting configuration until the virtual server or port does not have any active connections.

Example

The following command changes a virtual port's connection limit to 10000:

```
AX(config-slb virtual server-slb virtua...)#conn-limit 10000
```

def-selection-if-pref-failed

Description

Configure SLB to continue checking for an available server in other service groups if all of the servers are down in the first service group selected by SLB.

Syntax

```
[no] def-selection-if-pref-failed
```

Default

Enabled

Mode

Virtual port

Usage

During SLB selection of the preferred server to use for a client request, SLB checks the following configuration areas, in the order listed:

1. Layer 3-4 configuration items:
   a. aFleX policies triggered by Layer 4 events. (Not applicable to IPv6 migration releases.)
   b. Policy-based SLB (black/white lists). PBSLB is a Layer 3 configuration item because it matches on IP addresses in black/white lists. (Not applicable to IPv6 migration releases.)
2. Layer 7 configuration items:
   a. Cookie switching
   b. aFleX policies triggered by Layer 7 events (Not applicable to IPv6 migration releases.)
   c. URL switching
   d. Host switching

3. Default service group. If none of the items above results in selection of a server, the default service group is used.
   - If the configuration uses only one service group, this is the default service group.
   - If the configuration uses multiple service groups, the default service group is the one that is used if none of the templates used by the configuration selects another service group instead.

The first configuration area that matches the client or VIP (as applicable) is used, and the client request is sent to a server in the service group that is applicable to that configuration area.

When the def-selection-if-pref-failed option is enabled, SLB continues to check for an available server in other service groups if all servers are down in the first service group selected by SLB.

Example The following command enables this option:

```
AX(config-slb virtual server-slb virtua...)#def-selection-if-pref-failed
```

disable

Description Disable a virtual port.

Syntax `[no] disable`

Default Enabled

Mode Virtual port

Example The following command disables a virtual port:

```
AX(config-slb virtual server-slb virtua...)#disable
```

enable

Description Enable a virtual port.

Syntax `[no] enable`

Default Enabled

Mode Virtual port

Example The following command re-enables a virtual port:

```
AX(config-slb virtual server-slb virtua...)#enable
```

extended-stats

Description Enable collection of peak connection statistics for a virtual port.

Syntax `[no] extended-stats`

Default Disabled

Mode Virtual port

name

Description Change the name assigned to the virtual port.

Syntax `name string`

Parameter	Description
string	Name for the virtual port.

Default The AX device assigns a name that uses the following format:

_vip-addr_service-type_portnum

Mode Virtual port

Introduced in Release 2.6.6-P4

no-dest-nat

Description Disable destination NAT.

Syntax `[no] no-dest-nat`

Default Destination NAT is enabled by default.

Mode Virtual port

Usage Disabling destination NAT enables Direct Server Return (DSR).

In the current release, for IPv4 VIPs, DSR is supported on virtual port types (service types) TCP, UDP, FTP, and RTSP. For IPv6 VIPs, DSR is supported on virtual port types TCP, UDP, and RTSP.

VIP redistribution is not supported for VIPs on which destination NAT has been disabled. For example, VIP redistribution is not supported for VIPs that are configured for Direct Server Return (DSR).

Example The following command enables DSR:

```
AX(config-slb virtual server-slb virtua...)#no-dest-nat
```

service-group

Description Bind a virtual port to a service group.

Syntax

```
[no] service-group group-name
```

Parameter	Description
group-name	Service-group name.

Default N/A

Mode Virtual port

Usage The normal form of this command binds the virtual port to the specified service group. The “**no**” form of this command removes the binding.

One virtual port can be associated with one service group only, while one service group can be associated with multiple virtual ports.

The type of service group and type of virtual port should match. For example, a UDP service group can not be bound to an HTTP virtual port.

Example The following examples bind a service group to a virtual port, then remove the binding, respectively.

```
AX(config-slb virtual server-slb virtua...)#service-group tcp-grp
AX(config-slb virtual server-slb virtua...)#no service-group tcp-grp
```

snat-on-vip

Description Enable IP NAT support for the virtual port.

Syntax

```
[no] snat-on-vip
```

Default Disabled

Mode Virtual port

Usage Source IP NAT can be configured on a virtual port in the following ways:

1. ACL-based source NAT (**access-list** command at virtual port level)
2. VIP source NAT (**slb snat-on-vip** command at global configuration level)
3. aFleX policy (**aflex** command at virtual port level). (Not applicable to IPv6 migration releases.)
4. Non-ACL source NAT (**source-nat** command at virtual port level)

These methods are used in the order shown above. For example, if IP source NAT is configured using an ACL on the virtual port, and the **slb snat-on-vip** command is also used, then a pool assigned by the ACL is used for traffic that is permitted by the ACL. For traffic that is not permitted by the ACL, VIP source NAT can be used instead.

Note: The current release does not support source IP NAT on FTP or RTSP virtual ports.

source-nat

Description Enable source NAT. Source NAT is required if the real servers are in a different subnet than the VIP.

Note: This command is not applicable to the mms or rtsp service types.

Syntax

```
[no] source-nat pool
{pool-name | pool-group-name}
```

Sub-Command	Description
pool-name	Specifies the name of an IP pool of addresses to use as source addresses.
pool-group-name	Specifies the name of a group of IP address pools to use as source addresses.

Default Disabled.

Mode Virtual port

Usage By default, source NAT is disabled.

This command enables source NAT.

This command enables source NAT using a single NAT pool or pool group, for all source addresses. If you want the AX device to select from among multiple pools based on source IP address, configure policy-based source NAT instead. See “access-list” on page 651.

Example The following example enables source NAT for the virtual port:

```
AX(config-slb virtual server-slb virtua...)#source-nat pool pool2
```

stats-data-disable

Description Disable collection of statistical data for the virtual port.

Syntax `stats-data-disable`

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual port

stats-data-enable

Description Enable collection of statistical data for the virtual port.

Syntax `stats-data-enable`

Default Statistical data collection for load-balancing resources is enabled by default.

Mode Virtual port

Usage

To collect statistical data for a load-balancing resource, statistical data collection also must be enabled globally. (See "stats-data-enable" on page 184.)

template

Description

Applies an SLB configuration template to a virtual port.

Syntax

```
[no] template template-type template-name
```

Parameter	Description
template-type	Type of template. The template types that are available depend on the service type of the virtual port. To list the available template types, enter the following command: **template ?** For information about the **virtual-port** template type, see "template virtual-port" on page 661.
template-name	Name of the template.

Default

If the AX device has a default template that is applicable to the service type, the default template is automatically applied. The AX device has a default virtual-port template, which is applied to a virtual port when you create it.

Mode

Virtual port

Usage

The normal form of this command applies the specified template to the virtual port. The "**no**" form of this command removes the template from the virtual port but does not delete the template itself.

A virtual port can be associated with only one template of a given type. However, the same template can be associated with more than one virtual port.

To bind a virtual-port template to the port, see "template virtual-port" on page 661.

Example

The following example applies connection reuse template "reuse-template" to a virtual port:

```
AX(config-slb virtual server-slb virtua...)#template connection-reuse
reuse-template
```

template virtual-port

Description

Bind a a virtual service port template to the virtual port.

Syntax

```
[no] template virtual-port template-name
```

Default

The virtual port template named "default" is bound to virtual ports by default. The parameter settings in the default virtual port template are automatically applied to the new virtual port, unless you bind a different virtual port template to the virtual port.

Mode

Virtual port

Usage

If a parameter is set individually on this virtual port and also is set in a virtual port template bound to this virtual port, the individual setting on this port is used instead of the setting in the template.

To configure a virtual port template, see "slb template virtual-port" on page 637.

Example

The following commands configure a virtual service port template named "common-vpsettings", set the connection limit, and bind the template to a virtual port:

```
AX(config)#slb template virtual-port common-vpsettings
AX(config-Virtual port template)#conn-limit 500000
AX(config-Virtual port template)#exit
AX(config)#slb virtual-server vip1 10.10.10.99
AX(config-slb vserver)#port 80 http
AX(config-slb vserver-vport)#template virtual-port common-vpsettings
```

use-default-if-no-server

Description

Forward client traffic at Layer 3, if SLB server selection fails.

Syntax

```
[no] use-default-if-no-server
```

Default

Disabled. If SLB server selection fails, the traffic is dropped.

Mode

Virtual port

Usage

This command applies only to wildcard VIPs (VIP address 0.0.0.0).

use-rcv-hop-for-resp

Description

Force the AX Series device to send replies to clients back through the last hop on which the request for the virtual port's service was received.

Syntax

```
[no] use-rcv-hop-for-resp
```

Default

Disabled.

Mode

Virtual port

Usage

Last hop information is not included in the information sent to the Standby AX device during HA session synchronization. If an HA failover occurs, the last hop might not be used for the reply.

Example

The following command enables this option:

```
AX(config-slb virtual server-slb virtua...)#use-rcv-hop-for-resp
```

Config Commands: Health Monitors

The commands in this chapter configure server resource health monitors.

To access this configuration level, enter the **health monitor** *monitor-name* command at the global config level.

This CLI level also has the following commands, which are available at all configuration levels:

- **clear** – See “clear” on page 59.
- **debug** – See “debug” on page 64.
- **do** – See “do” on page 117.
- **end** – See “end” on page 123.
- **exit** – See “exit” on page 124.
- **no** – See “no” on page 155.
- **show** – See “Show Commands” on page 689.
- **write** – See “write terminal” on page 78.

disable-after-down

Description Disable the target of a health check if the target fails the health check.

Syntax

```
[no] disable-after-down
```

Default Disabled

Mode Health monitor configuration

Usage This command applies to all servers, ports, or service groups that use the health monitor. When a server, port, or service group is disabled based on this command, the server, port, or service group’s state is changed to **disable** in the running-config. If you save the configuration while the server, port, or service group is disabled, the state change is written to the startup-config.

The server, port, or service group remains disabled until you explicitly enable it.

method

Description

Configure a health method.

Syntax

```
[no] method method-options
```

method-options	Description
dns {*ipaddr* | **domain** *domain-name*} [*options*]	Sends a lookup request to the specified port number for the specified domain name. By default, expects reply with code 0. You can specify a domain name or a server IP address as the target of the health check. You also can configure the following options: **expect response-code** *code-list* – Specifies a list of response codes, in the range 0-15, that are valid responses to a health check. The DNS server can respond with any of the expected response codes. By default, the expect list is empty, in which case the AX device expects status code 0 (No error condition). **port** *port-num* – Specifies the protocol port number on which the DNS server listens for DNS queries. Use this option if the server is not using the default DNS port, 53. **recurse** {**enabled** | **disabled**} – Specifies whether the tested DNS server is allowed to send the health check's request to another DNS server if the tested server can not fulfill the request using its own database. Recursion is enabled by default. **type** {**A** | **CNAME** | **SOA** | **PTR** | **MX** | **TXT** | **AAAA**} – For health checks sent to a domain name, specifies the record type the responding server is expected to send in reply to health checks. You can specify one of the following record types: A – IPv4 address record

CNAME – Canonical name record for a DNS alias

SOA – Start of authority record

PTR – Pointer record for a domain name

MX – Mail Exchanger record

TXT – Text string

AAAA – IPv6 address record

By default, the AX device expects the DNS server to respond to the health check with an A record.

`external [port` *`port-num`*`]` **`program`** *`program-name`* `[`**`arguments`** *`argument-string`*`]`

Runs an external program (for example, a Tcl script) and bases the health status on the outcome of the program. See “Usage” below for more information on health check using an external program.

`icmp` `[`**`transparent`** *`ipaddr`*`]`

Sends an ICMP echo request to the server. Expects ICMP echo reply message.

The **transparent** *ipaddr* option applies only to specific configurations, where the health check must check the path through a device:

> In DSR, the *ipaddr* specifies the virtual IP address.
>
> In FWLB, the *ipaddr* specifies the IP address of the AX device on the other side of the firewall, or the floating IP address of the HA group on the other side of the firewall.

`udp port` *`port-num`*

Sends a packet with a valid UDP header and a garbage payload to the specified UDP port on the server. Expects either of the following:

– server reply from the specified UDP port, with any type of packet.

– server does not reply at all.

The server fails the health check only if the server replies with an ICMP Error message.

Default

The configuration has a default "ping" health monitor that uses the **icmp** method. The AX device applies the ping monitor by default. The AX device also applies the TCP or UDP health monitor by default, depending on the port type. These default monitors are used even if you also apply configured monitors to a service port.

To use differently configured ping or TCP/UDP monitors, configure new monitors with the ICMP, TCP, or UDP method and apply those monitors instead.

When specifying a protocol port number, specify the port number on the real server, not the port number of the virtual port. By default, the well-known port number for the service type of the health monitor is used. For example, for LDAP, the default port is 389 (or 636 if the **overssl** option is used).

If you specify the protocol port number in the health monitor, the protocol port number configured in the health monitor is used if you send an on-demand health check to a server without specifying the protocol port. (See "health-test" on page 52.) After you bind the health monitor to a real server port, health checks using the monitor are addressed to the real server port number instead of the port number specified in the health monitor's configuration. In this case, you can override the IP address or port using the **override** commands described later in this chapter.

Mode

Health monitor configuration

Usage

To use a health method, you must do the following:

1. Configure a health monitor, by assigning a name to it and by assigning one of the health methods listed above to it. Use the **health monitor** command at the global Config level to create and name the monitor. (See "health monitor" on page 128.) Use the **method** command at the monitor configuration level to assign a health method to the monitor.

Note: To configure a health monitor that uses a script, use the **health external** command to create it, instead of using the **health monitor** command. (See "health external" on page 126 and the external health check example below.)

2. Apply the health monitor to a real server or real server port, using the **health-check** command at the configuration level for the server or the server port. Apply monitors that use the ICMP method to real servers. Apply UDP monitors to individual server ports.

override-ipv4

Description

Send the health check to a specific IPv4 address, instead of sending the health check to the IP address of the real server to which the health monitor is bound. This command and the other override commands are particularly useful for testing the health of remote links.

Syntax

```
[no] override-ipv4 ipaddr
```

Default

By default, a health check is addressed to the real server IP address of the server to which the health monitor is bound.

Mode

Health monitor configuration

Example

The following commands configure a health monitor to check 192.168.1.1:

```
AX(config)#health monitor site1-hm
AX(config-health:monitor)#method icmp
AX(config-health:monitor)#override-ipv4 192.168.1.1
```

override-ipv6

Description

Send the health check to a specific IPv6 address, instead of sending the health check to the IP address of the real server to which the health monitor is bound.

Syntax

```
[no] override-ipv6 ipv6addr
```

Default

By default, a health check is addressed to the real server IP address of the server to which the health monitor is bound.

Mode

Health monitor configuration

Example

The following commands configure a health monitor to check 2001:db8::1521:31ab:

```
AX(config)#health monitor site2-hm
AX(config-health:monitor)#method icmp
AX(config-health:monitor)#override-ipv6 2001:db8::1521:31ab
```

override-port

Description

Send the health check to a specific protocol port, instead of sending the health check to the server port to which the health monitor is bound.

Syntax `[no] override-port portnum`

Default By default, a health check is addressed to the protocol port number to which the health monitor is bound.

Mode Health monitor configuration

Example The following commands configure a health monitor to check port 8081 on 192.168.1.1:

```
AX(config)#health monitor site3-hm
AX(config-health:monitor)#method http
AX(config-health:monitor)#override-ipv4 192.168.1.1
AX(config-health:monitor)#override-prt 8081
```

strictly-retry-on-server-error-response

Description Force the AX device to wait until all retries are unsuccessful before marking a server or port Down.

Syntax `[no] strictly-retry-on-server-error-response`

Default Disabled. For some health method types, the AX device marks the server or port Down after the first failed health check attempt, even if the retries option for the health monitor is set to higher than 0.

Mode Health monitor configuration

Usage This command is applicable only to some types of health monitors, such as HTTP health monitors. For example, this command applies to HTTP health monitors that expect a string in the server reply. By default, if the server’s HTTP port does not reply to the first health check attempt with the expected string, the AX device immediately marks the port Down.

Example The following commands configure an HTTP health monitor that checks for the presence of “testpage.html”, and enable strict retries for the monitor.

```
AX(config)#health monitor http-exhaust
AX(config-health:monitor)#method http url GET /testpage.html
AX(config-health:monitor)#strictly-retry-on-server-error-response
```

Config Commands: High Availability

The commands in this chapter configure global High Availability (HA) parameters. (Also see "floating-ip" on page 125.)

Note: This chapter provides reference information for individual commands. For information about how HA works and how to configure it, see the *AX Series System Configuration and Administration Guide*.

This CLI level also has the following commands, which are available at all configuration levels:

- **backup** – See "backup system" on page 50 and "backup log" on page 48.
- **clear** – See "clear" on page 59.
- **debug** – See "debug" on page 64.
- **do** – See "do" on page 117.
- **end** – See "end" on page 123.
- **exit** – See "exit" on page 124.
- **no** – See "no" on page 155.
- **show** – See "Show Commands" on page 689.
- **write** – See "write terminal" on page 78.

ha arp-retry

Description

Change the number of additional gratuitous ARPs, in addition to the first one, an AX sends after transitioning from Standby to Active in an HA configuration. These ARPs are sent at intervals of 500 milliseconds.

Syntax

```
[no] ha arp-retry num
```

Parameter	Description
num	Specifies the number of additional gratuitous ARPs to send, after sending the first one. You can specify 1-255.

Default

The AX device sends 4 additional gratuitous ARPs by default, for a total of 5.

Mode Configuration mode

Example The following command increases the number of additional gratuitous ARPs to 9, for a total of 10 ARPs:

```
AX(config)#ha arp-retry 9
```

ha check gateway

Description Configure an AX device to detect the status of its gateway routers, and change HA status based on gateway status changes.

Syntax

```
[no] ha check gateway ipaddr
```

Parameter	Description
ipaddr	IP address of the gateway.

Default Not set

Mode Configuration mode

Usage This feature uses health monitors to check the availability of the gateways. If any of the active AX device's gateways fails a health check, the AX device changes its HA status to Down. If the HA status of the other AX device is higher than Down, a failover occurs.

Likewise, if the gateway becomes available again and all gateways pass their health checks, the AX device recalculates its HA status according to the HA interface counts. If the new HA status of the AX device is higher than the other AX device's HA status, a failover occurs.

Configuration of gateway-based failover requires the following steps:

1. Configure a health monitor that uses the ICMP method. (See "health monitor" on page 128.)
2. Configure the gateway as an SLB real server and apply the ICMP health monitor to the server. (See "method" on page 664.)
3. Enable HA checking for the gateway, using the command described in this section.

Example The following commands configure gateway-based failover for gateway 10.10.10.1:

```
AX(config)#health monitor gatewayhm1
AX(config-health:monitor)#method icmp
AX(config-health:monitor)#exit
AX(config)#slb server gateway1 10.10.10.1
AX(config-real server)#health-check gatewayhm1
AX(config-real server)#exit
AX(config)#ha check gateway 10.10.10.1
```

ha check route

Description

Reduces the HA priority of all HA groups on the AX device, if the specified route is missing from the IPv4 or IPv6 route table.

Syntax

For IPv4 routes:

```
[no] ha check route destination-ipaddr /mask-
length
priority-cost weight
[gateway ipaddr]
[protocol {static | dynamic}]
[distance num]
```

For IPv6 routes:

```
[no] ha check route
destination-ipv6addr/mask-length
priority-cost weight
[gateway ipv6addr]
[protocol {static | dynamic}]
[distance num]
```

Parameter	Description
destination-ipaddr /mask-length	Specifies the destination IPv4 subnet of the route.
destination-ipv6addr/mask-length	Specifies the destination IPv6 address of the route.
priority-cost *weight*	Specifies the value to subtract from the HA priority of each HA group, if the IP route table does not have a route to the destination subnet.
gateway *ipaddr*	Specifies the next-hop gateway for the route.

protocol {static | dynamic}	Specifies the source of the route: **static** – The route was added by an administrator. **dynamic** – The route was added by a routing protocol. (This includes redistributed routes.)
distance *num*	Specifies the metric value (cost) of the route.

Default None

Mode Configuration mode

Usage This feature applies only to routes in the data route table. The feature does not apply to routes in the management route table.

For failover to occur due to HA priority changes, the HA pre-emption option must be enabled.

You can configure this option for up to 100 IPv4 routes and up to 100 IPv6 routes. This option is valid for all types of IP routes supported in this release (static and OSPF and IS-IS).

If the priority of an HA group falls below the priority for the same group on the other AX device in an HA pair, a failover can be triggered.

Omitting an optional parameter matches on all routes. For example, if you do not specify the next-hop gateway, routes that match based on the other parameters can have any next-hop gateway.

Example The following command configures HA route awareness for a default IPv4 route. If this route is not in the IP route table, 255 is subtracted from the HA priority of all HA groups.

```
AX(config)#ha check route 0.0.0.0 /0 priority-cost 255
```

Note: The lowest possible HA priority value is 1. Deleting 255 sets the HA priority value to 1, regardless of the original priority value.

Example The following command configures HA route awareness for a dynamic route to subnet 10.10.10.x with route cost 10. If the IP route table does not have a dynamic route to this destination with the specified cost, 10 is subtracted from the HA priority value for each HA group.

```
AX(config)#ha check route 10.10.10.0 /24 priority-cost 10 protocol dynamic dis-
tance 10
```

Example

The following commands configure HA route awareness for an IPv6 route to 3000::/64. Based on the combination of these commands, if the IPv6 route table does not contain any routes to the destination, 105 is subtracted from the HA priority of each HA group.

If the IPv6 route table does contain a static route to the destination, but the next-hop gateway is not 2001::1, the AX device subtracts only 5 from the HA priority of each HA group.

```
AX(config)#ha check route 3000::/64 priority-cost 100
AX(config)#ha check route 3000::/64 priority-cost 5 protocol static gateway
2001::1
```

ha check vlan

Description

Configure an AX device to detect the status of its VLANs, and change HA status based on VLAN status changes.

Syntax

`[no] ha check vlan vlan-id timeout seconds`

Parameter	Description
vlan-id	VLAN ID.
seconds	Number of seconds a VLAN can be inactive before a failover is triggered. The timeout can be 2-600 seconds. You must specify the timeout. Although there is no default, A10 recommends trying 30 seconds.

Default

Not set

Mode

Configuration mode

Usage

When HA checking is enabled for a VLAN, the active AX device in the HA pair monitors traffic activity on the VLAN. If there is no traffic on the VLAN for half the duration of a configurable timeout, the AX device attempts to generate traffic by issuing ping requests to servers if configured, or broadcast ARP requests through the VLAN.

If the AX device does not receive any traffic on the VLAN before the timeout expires, a failover occurs.

This HA checking method provides a passive means to detect network health, whereas heartbeat messages are an active mechanism. You can use either or both methods to check VLAN health. If you use both methods on a

VLAN, A10 recommends that you specify an HA checking interval (timeout) that is much longer than the heartbeat interval.

Example

The following command enables VLAN-based failover for VLAN 10 and sets the timeout to 30 seconds:

```
AX(config)#ha check vlan 10 timeout 30
```

ha conn-mirror

Description

Set the peer IP address to use for session synchronization (also called "connection mirroring") and config sync.

Syntax

```
[no] ha conn-mirror ip ipaddr
```

Parameter	Description
ipaddr	Specifies the IP address of a data interface on the other AX device in the HA configuration.

Default

None

Mode

Configuration mode

Usage

This command sets the IP address to which to mirror sessions. However, you also must use the **ha-conn-mirror** command on individual virtual ports to enable connection mirroring on the virtual ports.

Connection mirroring is required for config sync. Config sync uses the connection mirroring link.

HA session synchronization applies primarily to Layer 4 sessions. HA session synchronization does not apply to DNS sessions. Since these sessions are typically very short lived, there is no benefit to synchronizing them. Likewise, session synchronization does not apply to static NAT sessions. Synchronization of these sessions is not needed since the newly Active AX device will create a new flow for the session following failover.

Note: In HA deployments, the full-cone session age on the standby AX device is always 0.

Example

The following command sets the session synchronization address to 10.10.10.66, the IP address of the other AX in this HA pair:

```
AX(config)#ha conn-mirror ip 10.10.10.66
```

ha force-self-standby

Description Force HA groups to change from Active to Standby status.

Syntax

```
[no] ha force-self-standby [group-id]
```

Parameter	Description
group-id	Specifies the group ID. Only the specified group is forced to change from Active to Standby. If you do not specify a group ID, all Active groups are forced to change to Standby status.

Default N/A

Mode Configuration mode

Usage This command provides a simple method to force a failover, without the need to change HA group priorities and enable pre-emption. The command is not added to the configuration and does not persist across reboots.

Example The following command forces HA group 1 to change from Active to Standby status:

```
AX(config)#ha force-self-standby 1
```

ha forward-l4-packet-on-standby

Description Enable Layer 2/3 forwarding of Layer 4 traffic on the Standby AX device.

Syntax

```
[no] ha forward-l4-packet-on-standby
```

Default Disabled. Layer 4 traffic is dropped by the Standby AX device.

Mode Configuration mode

ha group

Description Configure an HA group and set its priority.

Syntax

```
[no] ha group group-id priority num
```

Parameter	Description
group-id	HA group ID, 1-31.
num	Number from 1 (low priority) to 255 (high priority).

Default

The configuration does not have a default HA group. HA groups do not have a default priority. You must set the priority.

Mode

Configuration mode

Usage

In Active-Standby configurations, configure only one HA group. Use the same group ID on each AX device.

In Layer 3 Active-Active configurations, to make one AX active for some virtual servers and make the other AX active for the other virtual servers, configure multiple HA groups and give them different priorities. Use the same group IDs for the same virtual servers on each AX.

Example

The following command configures HA group 1 and sets its priority to 100:

```
AX(config)#ha group 1 priority 100
```

ha id

Description

Enable HA.

Syntax

```
[no] ha id {1 | 2} [set-id num]
```

Parameter	Description
1 | 2	HA ID for the AX device.
set-id *num*	HA set ID, 1-7.

Default

Neither parameter is set.

Mode

Configuration mode

Usage

Use HA ID 1 on one of the AX Series devices in the HA pair. Use HA ID 2 on the other AX Series device in the HA pair.

The **set-id** option allows you to use multiple HA pairs. The set ID must be unique for each AX pair.

Example

The following command enables HA with ID 1:

```
AX(config)#ha id 1
```

ha interface

Description Configure an HA interface.

Syntax

```
[no] ha interface ethernet port-num
[redundant]
[router-interface | server-interface | both]
[no-heartbeat | vlan vlan-id]
```

Parameter	Description
port-num	Specifies the HA interface.
redundant	Identifies the link as secondary link, in terms of sending heartbeat messages. Normally, redundant links do not send heartbeat messages. (For more information, see the *AX Series System Configuration and Administration Guide*.)
router-interface | server-interface | both	Identifies the type of device connected to the HA interface: **router-interface** – The HA interface is connected to an upstream router. **server-interface** – The HA interface is connected to a real server. **both** – The HA interface is connected to an upstream router ***and*** a real server.
no-heartbeat | vlan *vlan-id*	Disables HA heartbeat messages on the HA interface, or enables them only on the specified VLAN. If the port is tagged and heartbeat messages are enabled, you must specify the VLAN.

Default No HA interfaces are set by default. When you set an HA interface, the device type is not set by default. Heartbeat messages are enabled on the interface by default.

Mode Configuration mode

Usage

At least one HA interface must be specified and at least one HA interface must have heartbeat messages enabled. If the interface is tagged, a VLAN ID must be specified if heartbeat messages are enabled on the interface.

Note: The maximum number of HA interfaces you can configure is the same as the number of Ethernet data ports on the AX device.

If the heartbeat messages from one AX device to the other will pass though a Layer 2 switch, the switch must be able to pass UDP IP multicast packets.

Set each interface connected to the real servers or clients (for example, connected through upstream routers) as an HA interface. Also set the interface that connects an AX Series device to its HA peer (the other AX device in the HA pair) as an HA interface.

Device Type Options

Setting the device type increases the granularity of the HA state.

- If the device type is not set, the HA state of the AX device can be one of the following:
  - Up – All configured interfaces are up.
  - Down – At least one of the HA interfaces is down.
- If you set the device type, the HA status of the AX device is based on the status of the AX link with the real server or upstream router:
  - Up – All configured HA router and server interfaces are up.
  - Partially Up – Some HA router or server interfaces are down but at least one server link and one router link are up.
  - Down – All router interfaces, or all server interfaces, or both are down. The status also is Down if neither router interfaces nor server interfaces are configured and an HA interface goes down.

  If both types of interfaces (router interfaces and server interfaces) are configured, the HA interfaces for which a type has not been configured are not included in the HA interface status determination.

Example

The following command configures Ethernet port 2 as an HA interface, indicates that it is connected to a router, and disables heartbeat messages on the interface:

```
AX(config)#ha interface ethernet 2 router-interface no-heartbeat
```

ha l3-inline-mode

Description

Enable blocking of traffic loops in a gateway (Layer 3) hot-standby HA configuration.

Syntax `[no] ha l3-inline-mode`

Default Disabled.

Mode Configuration mode

Usage Layer 3 inline support applies specifically to network topologies where inserting a pair of AX Series devices would cause a traffic loop. In this type of topology, Layer 3 inline mode enables you to deploy the AX Series devices in an HA pair without the need to change the network topology or enable Spanning Tree Protocol (STP) on any of the devices in the network.

Inline mode is designed for one HA group in Hot-Standby mode. Do not configure more than one HA group on an AX running in inline mode.

Example The following command enables Layer 3 inline mode:

```
AX(config)#ha l3-inline-mode
```

ha link-event-delay

Description Change the delay waited by the AX device before changing the HA state (Up, Partially Up, or Down) in response to link-state changes on HA interfaces.

Syntax `[no] ha link-event-delay 100-ms-unit`

Parameter	Description
100-ms-unit	Specifies how many 100-ms units (one tenth of a second units) to use for the delay. You can set the delay to a value from 100 milliseconds (ms) to 10000 ms, in increments of 100 ms.

Default 3000 ms (3 seconds)

Mode Configuration mode

Usage This command applies only to inline mode. The delay is applicable in the following situations:

- The AX device is Active and a link goes down.
- The AX device is Standby and a link comes up. (There is an additional 10-20 second delay in this case.)

The delay helps prevent HA flapping.

Example The following command changes the HA state change delay to 5 seconds:

```
AX(config)#ha link-event-delay 50
```

ha ospf-inline vlan

Description In HA Layer 3 inline mode, leave OSPF enabled on the Standby AX device, on the specified VLAN.

Syntax

```
[no] ha ospf-inline vlan vlan-id
```

Default Enabled for all VLANs.

Mode Configuration mode

Usage When this option is enabled, OSPF on the Standby AX device will always participate in OSPF routing. There is no additional time gap when failover happens.

To limit OSPF adjacency formation to a specific VLAN only, explicitly configure adjacency formation for that VLAN. In this case, OSPF adjacency formation does not occur for any other VLANs.

ha preemption-enable

Description Allow the high-priority HA group to take over from the currently active one. This command enables you to force HA failovers based on HA configuration changes.

Syntax

```
[no] ha preemption-enable
```

Default Pre-emption is disabled by default. By default, a failover occurs only in the following cases:

- The Standby AX device stops receiving HA heartbeat messages from the other AX device in the HA pair.
- The HA interface state changes give the Standby AX device a better HA state than the Active AX device.

By default, failover ***does not*** occur due to HA configuration changes to the HA priority.

Note: To force failover without changing HA group priorities or enable preemption, see “ha force-self-standby” on page 675.

Mode Configuration mode

Example The following command enables HA pre-emption mode:

```
AX(config)#ha preemption-enable
```

ha restart-port-list

Description Configure HA interfaces on the previously Active AX device to toggle (shut down and restart) following HA failover.

Syntax

```
[no] ha restart-port-list ethernet port-list
```

Parameter	Description
port-list	Specifies the HA interfaces to restart.

Note: You must omit at least one port connecting the AX devices from the restart port-list, and heartbeat messages must be enabled on the port. This is so that heartbeat messages between the AX devices are maintained; otherwise, flapping might occur.

Note: On model AX 2000 or AX 2100, A10 recommends that you do not include Fiber ports in the restart port list.

Default Disabled. HA interfaces are not restarted after a failover.

Mode Configuration mode

Usage Use this command in inline mode configurations to cause the router connected to the AX Series 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 AX Series device that becomes the Standby AX device after a failover.

HA port restart toggles a specified set of ports on the formerly Active AX 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 AX.

Example The following command enables restart of HA interfaces 1 and 2, to occur if the AX Series device transitions to Standby:

```
AX(config)#ha restart-port-list ethernet 1 to 2
```

ha restart-time

Description

Configure the amount of time HA interfaces remain disabled following a failover.

Syntax

```
[no] ha restart-time 100-msec-units
```

Parameter	Description
100-msec-units	Amount of time to keep the HA interfaces disabled. You can specify 1-100 units of 100 ms (from 0.1 seconds to 10 seconds).

Default

The default is 20 units of 100 milliseconds (ms) each, for a total of 2 seconds.

Mode

Configuration mode

Usage

This command applies only to HA interfaces in a restart port list configured by the **ha restart-port-list** command. (See "ha restart-port-list" on page 681.)

Example

The following command changes the restart interval to 4 seconds:

```
AX(config)#ha restart-time 40
```

ha start-redundant-msg-count

Description

Configure the trigger to begin sending HA heartbeat messages on backup (redundant) HA interfaces.

Syntax

```
[no] ha start-redundant-msg-count num
```

Parameter	Description
num	Specifies the maximum number of consecutive HA heartbeat messages that can be missing on any primary (non-redundant) HA interface before the AX device starts sending heartbeat messages on the redundant (backup) HA interfaces. You can specify 2-255 missing heartbeat messages.

Default

2

Mode

Configuration mode

Usage

The AX device can be an initiator or a receiver of HA heartbeat messages.

- Initiator – The AX device becomes an initiator of heartbeat messages on redundant HA interfaces, if the AX device does not receive the specified number of consecutive heartbeat messages, on any of the primary HA interfaces.
- Receiver – The AX device becomes a receiver of heartbeat messages on redundant HA interfaces, if the AX device receives a heartbeat message on any redundant HA interface.

Once transmission of heartbeat packets on redundant HA interfaces is triggered, the AX device continues sending heartbeat messages to the redundant HA interfaces until any of the following occurs:

- If an initiator, the AX device receives at least the minimum number of heartbeat messages specified by **stop-redundant-msg-count**, on each primary HA interface. (See “ha stop-redundant-msg-count” on page 683.)
- If a receiver, the AX device stops receiving heartbeat messages from the other AX device on the redundant HA interfaces.

To stop sending heartbeat messages on redundant HA interfaces, the AX device must not be an initiator or a receiver of heartbeat messages on any redundant HA interfaces.

ha stop-redundant-msg-count

Description

Configure the trigger to stop sending HA heartbeat messages on backup (redundant) HA interfaces.

Syntax

```
[no] ha stop-redundant-msg-count num
```

Parameter	Description
num	Specifies the minimum number of consecutive HA heartbeat messages that must be received from the other AX device on each of the primary HA interfaces, before the AX device stops sending heartbeat messages on the redundant (backup) HA interfaces. You can specify 2-255 missing heartbeat messages.

Default

5

Mode

Configuration mode

Syntax See “ha start-redundant-msg-count” on page 682.

ha sync

Description Synchronize the Layer 4-7 configuration information of the standby AX Series device with the active AX device in an HA pair.

Syntax

```
ha sync all
{to-startup-config [with-reload] |
  to-running-config} ipaddr
```

Syntax

```
ha sync startup-config
{to-startup-config [with-reload] |
  to-running-config} ipaddr
```

Syntax

```
ha sync running-config
{to-startup-config [with-reload] |
  to-running-config} ipaddr
```

Syntax

```
ha sync data-files ipaddr
```

Parameter	Description
`all`	Synchronizes data files and the running-config. (See “Usage” for a list of the types of data files that are synchronized.) You can synchronize the running-config to one of the following on the other AX Series device: **`startup-config`** – Replaces the startup-config on the other AX device with the running-config on this device. For information about the **with-reload** option, see “Usage” below.

Note: If the HA status is Standby for all the HA groups on the other AX device, the AX device is reloaded anyway, even if the **with-reload** option is not used.

Parameter	Description
	`running-config` – Replaces the running-config on the other AX device with the running-config on this device.
`data-files`	Synchronizes data files but not the running-config or startup-config. (See “Usage” for a list of the types of data files that are synchronized.)

`running-config` Synchronizes the running-config. You can synchronize it to one of the following on the other AX Series device:

`startup-config` – Replaces the startup-config on the other AX device with the running-config on this device. For information about the **with-reload** option, see “Usage” below.

`running-config` – Replaces the running-config on the other AX device with the running-config on this device.

`startup-config` Synchronizes the startup-config. See above for descriptions of the options. You can synchronize it to one of the following on the other AX Series device:

`startup-config` – Replaces the startup-config on the other AX device with the startup-config on this device. For information about the **with-reload** option, see “Usage” below.

`running-config` – Replaces the running-config on the other AX device with the startup-config on this device.

`ipaddr` Specifies the IP address of the target AX device.

Default N/A

Mode Configuration mode

Usage Connection mirroring is required for config sync. Config sync uses the connection mirroring link. (See “ha conn-mirror” on page 674.)

SSH management access must be enabled on both ends of the link. (See “enable-management” on page 121.)

The following configuration items are backed up during HA config sync:

- Admin accounts and settings
- Floating IP addresses
- IP NAT configuration
- Access control lists (ACLs)
- Health monitors
- Server resources (real servers, service groups, virtual servers, and templates)

- Data Files:
  - External health check files
  - SSL certificate and private-key files

The following configuration items are ***not*** backed up during HA config sync:

- Management access settings (the ones described in “enable-management” on page 121)
- AX Hostname
- MAC addresses
- Management IP addresses
- Trunks or VLANs
- Interface settings
- RIP, OSPF, IS-IS, and BGP settings
- ARP entries or settings

This command does not have a “no” form.

Reload of the target AX device following synchronization

In certain cases, the target AX device is automatically reloaded, but in other cases, reload is either optional or is not allowed.

Table 30 lists the cases in which reload is automatic, optional, or not allowed.

TABLE 30 Reload of Target AX Device After Config-Sync

Admin Role	Status of Target AX	Target Config	Reload?
Root or Super User (Read-Write)	Standby	startup-config	Automatic
		running-config	Automatic
	Active	startup-config	Optional[1] Not reloaded by default
		running-config	Automatic

[1] If the target AX device is not reloaded, the GUI Save button on the Standby AX device does not blink to indicate unsaved changes. It is recommended to save the configuration if required to keep the running-config before the next reboot.

Data that is synchronized from a Standby AX device to an Active AX device is not available on the Active AX device until that device is rebooted or the software is reloaded.

Example

The following command synchronizes the running-config and data files by copying them from this AX Series device to the other one in the HA pair. The running-config is copied to the other AX device's startup-config, and the other AX device is then reloaded:

```
AX(config)#ha sync all startup-config 10.10.10.77
User name []?admin
Password []?***
```

ha time-interval

Description

Configure the interval between HA heartbeat messages.

Syntax

```
[no] ha time-interval 100-msec-units
```

Parameter	Description
100-msec-units	Amount of time between sending each heartbeat message. You can specify 1-255 units of 100 ms each.

Default

200 milliseconds

Mode

Configuration mode

Example

The following command changes the HA time interval to 400 ms:

```
AX(config)#ha time-interval 4
```

ha timeout-retry-count

Description

Configure the number of HA heartbeat intervals the Standby AX Series device will wait for a heartbeat message from the Active AX device before failing over.

Syntax

```
[no] ha timeout-retry-count num
```

Parameter	Description
num	Number of times the HA time interval can expire before the Standby AX device fails over to become the Active AX device. You can specify 2-255.

Default 5

Mode Configuration mode

Example The following command changes the HA timeout retry count to 10:

```
AX(config)#ha timeout-retry-count 10
```

Show Commands

The **show** commands display configuration and system information.

In addition to the command options provided with some **show** commands, you can use output modifiers to search and filter the output. See “Searching and Filtering CLI Output” on page 42.

To automatically re-enter a **show** command at regular intervals, see “repeat” on page 74.

Also see the following:

- “LSN Show Commands” on page 485
- “DS-Lite Show Commands” on page 559
- “DNS64 / NAT64 Show Commands” on page 539

High Control CPU Utilization After Entering show CommandS

After entering a show command that results in a very large amount of output, control CPU utilization can reach 100%. To avoid this potential inconvenience, use the following command at the global configuration level of the CLI: **`system module-ctrl-cpu low`**

(See “system module-ctrl-cpu” on page 186.)

show 6rd

Description Display information for IPv6 Rapid Deployment (6rd). See “6rd Show Commands” on page 589.

show access-list

Description Display the configured Access Control Lists (ACLs). The output lists the configuration commands for the ACLs in the running-config.

Syntax

```
show access-list [ipv4 | ipv6] [acl-id]
```

Parameter	Description
ipv4 | ipv6	IP address type.
acl-id	ACL name or number.

Mode All

Example The following command displays the configuration commands for ACL 1:

```
AX#show access-list ipv4 1
access-list 1 permit 198.162.11.0 0.0.0.255  Hits: 3
access-list 1 deny 198.162.12.0 0.0.0.255  Hits: 1
```

Note: The ACL Hits counter is not applicable to ACLs applied to the management port.

show admin

Description Display the administrator accounts.

Syntax `show admin [admin-name] [detail | session]`

Parameter	Description
admin-name	Administrator name.
detail	Shows detailed information about the admin account.
session	Shows the current management sessions.

Mode Privileged EXEC mode and configuration mode

Example The following command lists the admins configured on an AX device:

```
AX(config)#show admin
UserName                      Status    Privilege
-------------------------------------------------------
admin                         Enabled   R/W
admin2                        Enabled   R
```

Table 31 describes the fields in the command output.

TABLE 31 show admin fields

Field	Description
UserName	Name of the AX admin.
Status	Administrative status of the account.

TABLE 31 show admin fields (Continued)

Field	Description
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.

Example

The following command lists details for the “admin” account:

```
AX#show admin admin detail
  User Name             ...... admin
  Status                ...... Enabled
  Privilege             ...... R/W
  Access type             .....cli web axapi
  GUI role            ......
  Trusted Host(Netmask) ...... Any
  Lock Status           ...... No
  Lock Time             ......
  Unlock Time           ......
  Password Type         ...... Encrypted
  Password              ...... $1$6334ba07$CKbWL/LuSNdY12kcE.KdS0
```

Table 32 describes the fields in the command output.

TABLE 32 show admin detail fields

Field	Description
User Name	Name of the AX 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.
Access type	Management interfaces the admin is allowed to access, which can be one or more of the following: • cli • web • axapi (not applicable to IPv6 migration)

TABLE 32 show admin detail fields (Continued)

Field	Description
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.
Password Type	Indicates whether the password is encrypted when displayed in the CLI or GUI and in the startup-config and running-config.
Password	The admin's password.

Example

The following command lists all the currently active admin sessions:

```
AX#show admin session
Id    User Name   Start Time                       Source IP       Type  Authen  Role
Cfg
------------------------------------------------------------------------------------
------------
*91    admin       18:03:03 GMT Thu Jan 27 2011   192.168.32.162   CLI   Local   Read-
WriteAdmin  No
```

Table 33 describes the fields in the command output.

TABLE 33 show admin session fields

Field	Description
Id	Admin session ID assigned by the AX device. The ID applies only to the current session.
User Name	Admin name.
Start Time	System time when the admin logged onto the AX 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.
Authen	Indicates the database used to authenticate the admin: • Local – Admin database on the AX device • RADIUS – Admin database on a RADIUS server • TACACS – Admin database on a TACACS+ server

TABLE 33 show admin session fields (Continued)

Field	Description
Role	Indicates the 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.
Cfg	Indicates whether the admin is at the configuration level.

show arp

Description

Display ARP table entries.

Syntax

```
show arp [all | ipaddr]
```

Mode

All

Example

The following command lists the ARP entry for host 192.168.1.144:

```
AX#show arp 192.168.1.144
Total arp entries: 1            Age time: 300 secs
IP Address         MAC Address          Type         Age  Interface    Vlan
---------------------------------------------------------------------------
192.168.1.144      0011.2F7C.1A75       Dynamic      293  Management   1
```

Table 34 describes the fields in the command output.

TABLE 34 show arp fields

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	For dynamic entries, the number of seconds since the entry was last used.
Interface	AX interface through which the device that has the displayed MAC address and IP address can be reached.
Vlan	VLAN through which the device that has the MAC address can be reached.

show audit

Description Show the command audit log.

Syntax

```
show audit
```

Mode All

Usage The audit log is maintained in a separate file, apart from the system log.

show axdebug file

Description Display AX debug capture files or their contents.

Syntax

```
show axdebug file [filename]
```

Mode All

Example The following command displays the list of AX debug capture files on the device:

```
AX(axdebug)#show axdebug file
------------------------------------+--------------+---------------------------
Filename                            |   Size(Byte) | Date
------------------------------------+--------------+---------------------------
file1                               |        58801 | Tue Sep 23 22:49:07 2008
file123                             |          192 | Fri Sep 26 17:06:51 2008
------------------------------------+--------------+---------------------------
Total: 2
Maximum file number is: 100
```

Example The following command displays the packet capture data in file “file123”:

```
AX(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 Display the configured AXdebug output filters.

Syntax

```
show axdebug filter [filter-num]
```

Mode All

show axdebug status

Description Display per-CPU packet capture counts for AXdebug.

Syntax

```
show axdebug status [cpu-num [...]]
```

Mode All

show backup

Description Display information about scheduled backups.

Syntax

```
show backup
```

Mode All

show bfd

Description Show information for

Syntax

```
show bfd {neighbors | statistics}
```

Option	Description
neighbors	Displays BFD neighbor information.
statistics	Displays BFD statistics.

Mode All

Example

The following command shows BFD neighbor information:

```
AX(config)#show bfd neighbors
Our Address    Neighbor Address        State       Holddown txint mult diag
219.0.0.1    219.0.0.2                 Up            150       50      3 3/0
219.0.1.1    219.0.1.2                 Up            150       50      3 3/0
219.0.2.1    219.0.2.2                 Up            150       50      3 0/0
219.0.3.1    219.0.3.2                 Up            150       50      3 0/0
219.0.4.1    219.0.4.2                 Up            150       50      3 3/0
219.0.5.1    219.0.5.2                 Up            150       50      3 3/0
219.0.6.1    219.0.6.2                 Up            150       50      3 0/0
219.0.7.1    219.0.7.2                 Up            150       50      3 3/0
```

Table 35 describes the fields in the command output.

TABLE 35 show bfd neighbors fields

Field	Description
Our Address	AX interface associated with the BFD session.
Neighbor Address	Neighbor interface associated with the BFD session.
State	Shows the state for each side of the session: *Local-state/Remote-state* For each side of the session, the state can be one of the following: • Init • Up • AdminDown • Down
Holdtime	Maximum amount of time the AX device waits for a BFD control packet from the neighbor.
txint	Configured interval at which the AX device sends BFD control packets to the neighbor.
mult	Maximum number of consecutive times the AX device will wait for a BFD control packet from the neighbor.
diag	Diagnostic codes for the local and remote ends of the BFD session. For information, contact A10 Networks.

Example

The following command shows BFD statistics:

```
AX(config)#show bfd statistics
IP Checksum error                        0
UDP Checksum error                       0
```

```
No session found with your_discriminator 0
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             0
BFD Packet auth seq# invalid             0
BFD Packet auth failed                   0
BFD local state is AdminDown             0
BFD Destination unreachable              0
BFD Other error                          0
```

Table 36 describes the fields in the command output.

TABLE 36 show bfd statistics fields

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 AX device.
Multihop config mismatch	Number of BFD packets whose multihop config did not match the BFD multihop config on the AX device.
BFD Version mismatch	Number of BFD packets with a different BFD version than the one in use by the AX device.
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	Number of BFD packets whose Length field value in the UDP header was shorter than the UDP header size plus the BFD Length value.

TABLE 36 show bfd statistics fields (Continued)

Field	Description
BFD Packet DetectMult is invalid	Number of BFD packets with an invalid detection time multiplier value.
BFD Packet Multipoint is invalid	Number of BFD packets with an invalid Multipoint setting.
BFD Packet my_discriminator is invalid	Number of BFD packets whose My Discriminator value was invalid.
BFD Packet TTL/Hop Limit is invalid	Number of BFD packets whose Time to Live or Hop Limit was invalid.
BFD Packet authentication length is invalid	Number of BFD packets whose authentication length was invalid.
BFD Packet authentication mismatch	Number of BFD packets whose authentication type did not match the BFD authentication type on the AX device.
BFD Packet authentication type mismatch	Number of BFD packets whose authentication type did not match the BFD authentication type on the AX device.
BFD Packet authentication key ID mismatch	Number of BFD packets whose authentication key ID did not match the BFD authentication key ID on the AX device.
BFD Packet authentication sequence number invalid	Number of BFD packets whose authentication sequence number was invalid.
BFD Packet authentication failed	Number of BFD packets with an incorrect authentication value.
BFD local state is AdminDown	Number of BFD packets received while the BFD session was administratively down.
BFD Destination unreachable	Number of times the destination IP address for a BFD neighbor was unreachable while the AX device 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 bgp

Description

Display information for Border Gateway Protocol (BGP). See “BGP Show Commands” on page 432.

show bootimage

Description Display the software images stored on the AX Series device.

Syntax **show bootimage**

Mode All

Example The following command shows the software images on an AX Series device:

```
AX#show bootimage
                      (* = Default)
                          Version
-----------------------------------------------
Hard disk primary         1.2.0.153 (*)
Hard disk secondary       1.2.1.24
Compact flash primary     1.1.1.68 (*)
Compact flash secondary   1.1.1.51
```

The asterisk (*) indicates the default image for each boot device (hard disk and compact flash). The default image is the one that the AX Series device will try to use first, if trying to boot from that boot device. (The order in which the AX tries to use the image areas is controlled by the **bootimage** command. See “bootimage” on page 105.)

show bpdu-fwd-group

Description Display the configured BPDU forwarding groups.

Syntax **show bpdu-fwd-group** [*number*]

Option	Description
number	Displays 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:

```
AX#show bpdu-fwd-group
BPDU forward Group 1 members:  ethernet 1 to 3
BPDU forward Group 2 members:  ethernet 9 to 12
```

show bridge-vlan-group

Description Display information for a bridge VLAN group.

Syntax

```
show bridge-vlan-group [group-id]
```

Mode All

show class-list

Description Display information for IP class lists.

Syntax

```
show class-list [name [ipaddr]]
```

Parameter	Description
name [*ipaddr*]	Specifies the class list name or an IP address in the class list. If you omit both options, the list of configured class lists is displayed instead.

Mode All

Example The following command displays the class-list files on the AX device:

```
AX#show class-list
Name                              IP       Subnet   Location
test                              4        3        file
user-limit                        14       4        config
Total: 2
```

Table 33 describes the fields in the command output.

TABLE 37 show class-list fields

Field	Description
Name	Name of the class list.
IP	Number of host IP addresses in the class list.
Subnet	Number of subnets 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 AX device.

show clns

Description

Show Connectionless Network Service (CLNS) information.

Syntax

```
show clns [tag]
[is-neighbors options | neighbors options]
```

Parameter	Description
`is-neighbors`	Displays IS neighbor adjacencies.
`neighbors`	Displays CLNS neighbor adjacencies.
`options`	Optional display filters: **detail** **ethernet** *portnum* [**detail**] **loopback** [*portnum*] [**detail**] **management** [**detail**] **trunk** *num* [**detail**] **udld** *num* [**detail**] **ve** *ve-num* [**detail**]

Mode

All

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 user configuration

Mode

All

Example

The following command shows clock information for an AX Series device:

```
AX#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 AX Series 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.

```
AX#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.

```
AX#show clock
*20:27:16 Europe/Dublin Sat Apr 28 2007
```

show core

Description Display core dump statistics.

Syntax `show core [process]`

Parameter	Description
process	Shows core dump statistics for AX processes. 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:

```
AX#show core
It has been rebooted 1 time.
It has been crashed 0 time.
The process is up 71048 sec.
```

show cpu

Description Display CPU statistics.

Syntax `show cpu [interval seconds]`

Parameter	Description
interval *seconds*	Automatically refreshes the output at the specified interval. If you omit this option, the output is shown one time. If you use this option, the output is repeatedly refreshed at the specified interval until you press ctrl+c.

Mode

Privileged EXEC level and configuration levels

Example

The following command shows CPU statistics on an AX 2000, in 10-second intervals:

```
AX#show cpu interval 10
Cpu Usage: (press ^C to quit)
            1Sec    5Sec    10Sec   30Sec   60Sec
--------------------------------------------------------
Time: 16:28:57 PST Wed Jan 16 2008
Control        2%      2%      2%      2%      2%
Data0          0%      0%      0%      0%      0%
Data1          0%      0%      0%      0%      0%

Time: 16:29:07 PST Wed Jan 16 2008
Control        2%      2%      2%      2%      2%
Data0          0%      0%      0%      0%      0%
Data1          0%      0%      0%      0%      0%
...
<ctrl+c>

AX#
```

Table 38 describes the fields in the command output.

TABLE 38 show cpu fields

Field	Description
Time	System time when the statistics were gathered.
Control	Control CPU.
Data0-7	Data CPU. The number of data CPUs depends on the AX model.
1Sec-60sec	Time intervals at which statistics are collected.

show debug

Description

This command applies to debug output. It is recommended to use the AXdebug subsystem commands instead of the debug commands. See the following:

- “AX Debug Commands” on page 789
- “show axdebug file” on page 694
- “show axdebug filter” on page 695
- “show axdebug status” on page 695

show disk

Description Display status information for the AX hard disks.

Syntax `show disk`

Mode Privileged EXEC level and configuration levels

Example The following command shows hard disk information for an AX Series device:

```
AX#show disk
  Total(MB)  Used       Free       Usage
-----------------------------------------
  154104     5895       148209     4.0%

  Device   Primary Disk        Secondary Disk
----------------------------------------------
  md0      Active              Active
  md1      Active              Active
```

Table 39 describes the fields in the command output.

TABLE 39 show disk fields

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 AX 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 your A10 Networks representative. • 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

Description Show DNS statistics.

Syntax **`show dns statistics`**

Mode Privileged EXEC level and configuration levels

Example The following command displays DNS statistics:

```
AX#show dns statistics
DNS statistics for SLB:
-----------------------
No. of requests: 510
No. of responses: 508
No. of request retransmits: 0
No. of requests with no response: 2
No. of responses with no matching session: 0
No. of resource failures: 0
DNS statistics for IP NAT:
--------------------------
No. of requests: 0
No. of responses: 0
No. of request retransmits: 0
No. of requests with no response: 0
No. of responses with no matching session: 0
No. of resource failures: 0
```

Note: In the current release, the “Response with multiple answers” and “Response with Short TTL” fields are not applicable and always contain 0.

show dns cache

Description Display DNS caching information.

Syntax

```
show dns cache {client | entry | statistics}
```

Parameter	Description
`client`	DNS client statistics.
`entry`	DNS cache entries.
`statistics`	DNS caching statistics.

Mode All

Example The following command shows DNS caching statistics:

```
AX#show dns cache statistics
Total allocated: 0
Total freed: 0
Total query: 100
Total server response: 55
Total cache hit: 49
Query not passed: 0
Response not passed: 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
Current allocate: 0
Current data allocate: 0
```

Table 40 describes the fields in the command output.

TABLE 40 show dns cache statistics fields

Field	Description
Total Allocated	Total memory allocated for cached entries.
Total Freed	Total memory freed.
Total Query	Total number of DNS queries received by the AX device.

TABLE 40 show dns cache statistics fields (Continued)

Field	Description
Total Server Response	Total number of responses form DNS servers received by the AX device.
Total Cache Hit	Total number of times the AX device was able to use a cached reply in response to a query.
Query Not Passed	Number of queries that did not pass a packet sanity check.
Response Not Passed	Number of responses that did not pass a packet sanity check. The AX device checks the DNS header and question in the packet, but does not parse the entire packet.
Query Encoded	Number of queries that were not cached because the domain name in the question was encoded in the DNS query packet.
Response Encoded	Number of queries that were not cached because the domain name in the question was encoded in the DNS response packet.
Query With Multiple Questions	Number of queries that were not cached because they contained multiple questions.
Response With Multiple Questions	Number of responses that were not cached because they contained answers for multiple questions.
Response With Multiple Answers	Number of responses that were not cached because they contained more than one answer.
Response with Short TTL	Number of responses that had a short time to live (TTL).
Total Aged Out	Total number of DNS cache entries that have aged out of the cache.
Total Aged for Lower Weight	Number of cache entries aged out due to their weight value.
Total Stats Log Sent	Total number of logs sent.
Current Allocate	Current memory allocation.
Current Data Allocate	Current data allocation.

show dns64

Description

Show information for DNS64. See “DNS64 / NAT64 Show Commands” on page 539.

show ds-lite

Description Show information for Dual-stack Lite (DS-Lite). See "DS-Lite Show Commands" on page 559.

show dumpthread

Description Show status information about the SLB process.

Syntax

```
show dumpthread
```

Mode Privileged EXEC level and configuration levels

Example The following command shows status information for the SLB process:

```
AX#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 AX Series device:

```
AX#show environment
Physical System temperature: 56C / 132F
Fan1 speed: 2576 RPM
Fan2 speed: 2576 RPM
Fan3 speed: 2576 RPM
Upper Power Unit State: On
Lower Power Unit State: On
```

show errors

Description

Show error information for the system. This command provides a simple way to quickly view system status and error statistics.

Syntax

```
show errors
[
application [sub-options] |
critical [detail] |
detail |
informational [detail] |
system [sub-options]
]
```

Option	Description
application [*sub-options*]	Displays error information for AX applications. The following *sub-options* are available. **critical** [**detail**] **detail** **ha** [**critical** [**detail**]] [**detail**] [**informational** [**detail**]] **hw-compression** [**critical** [**detail**]] [**detail**] [**informational** [**detail**]] **informational** [**detail**] **ipnat** [**critical** [**detail**]] [**detail**] [**informational** [**detail**]] **l2-l3-forward** [**critical** [**detail**]] [**detail**] [**informational** [**detail**]]

```
ram-cache

   [critical [detail]]
   [detail]
   [informational [detail]]

slb

   [critical [detail]]

   [detail]

   [health-monitor
     [critical [detail]]
     [detail]
     [informational [detail]]

   [informational [detail]]

   [layer4
     [critical [detail]]
     [detail]
     [informational [detail]]
     [tcp
       [critical [detail]]
       [detail]
       [informational [detail]]
     [udp
       [critical [detail]]
       [detail]
       [informational [detail]]

   [layer7
     [critical [detail]]
     [detail]
     [fast-http
       [critical [detail]]
       [detail]
       [informational [detail]]
     [http
       [critical [detail]]
       [detail]
       [informational [detail]]
     [informational [detail]]
     [sip
       [critical [detail]]
       [detail]
       [informational [detail]]
     [smtp
       [critical [detail]]
       [detail]
       [informational [detail]]
```

```
 [ssl-slb
  [critical [detail]]
  [detail]
  [informational [detail]]
[persist
 [cookie
  [critical [detail]]
  [detail]
  [informational [detail]]
 [critical [detail]]
 [dest-ip
  [critical [detail]]
  [detail]
  [informational [detail]]
 [detail]
 [informational [detail]
 [source-ip
  [critical [detail]]
  [detail]
  [informational [detail]]
 [ssl-sid
  [critical [detail]]
  [detail]
  [informational [detail]]
 [url-hash
  [critical [detail]]
  [detail]
  [informational [detail]]
ssl
[critical [detail]]
[detail]
[informational [detail]]
```

critical [detail]	Displays information about critical errors only.
detail	Displays detailed error information only.
informational [detail]	Displays informational output only.
system [*sub-options*]	Displays system-level errors. The following *sub-options* are available. **critical [detail]** **detail**

hardware

[**critical** [**detail**]]
[**detail**]
[**informational** [**detail**]]

informational [**detail**]

software

[**critical** [**detail**]]
[**detail**]
[**informational** [**detail**]]

Mode All

Example The following shows high-level error information for the system:

```
AX#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:

```
AX#show errors system software detail

System software Error Counters
==========================================
buff alloc failed:            : 0
buff alloc from sys failed:   : 0
Error packets drops:          : 16
Packet drops:                 : 0
```

Example The following command shows detailed error statistics for SLB health monitoring:

```
AX#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 AX 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 fixed-nat

Description Display information for Fixed-NAT. (See “Config Commands: Fixed-NAT” on page 609.)

show glid

Description Show information for global IP limiting rules.

Syntax **show glid** [*num*]

Mode All

show ha

Description

Show the status of each HA group. The output shows information for the AX device on which you enter the command, and the device's HA peer.

Syntax

```
show ha [config | detail]
```

Parameter	Description
`config`	Shows the HA configuration commands in the running-config.
`detail`	Shows HA statistics.

Mode

All

Example

The following command shows basic HA information:

```
AX#show ha
Local Unit:     UP              Peer Unit:      UP
HA Group        Unit            State           Priority
1               Local           Active          200
                Peer            Standby         100
2               Local           Active          255
                Peer            Standby         100
```

Example

The following command shows basic HA information along with HA statistics:

```
AX#show ha detail

Local Unit:     DOWN            Peer Unit:      ---
HA Group        Unit            State           Priority
1               Local           Active          255
                Peer            --              --

HA Group                        Active          Standby
1               Transitions     1               1

Connectivity:        Server Ports      0         Router Ports   0
HA packets:          Sent              0         Received       0
Conn Sync:           Sent              0         Received       0
Conn Query:          Sent              0         Received       0

Conn Sync Create Session:        Sent       0         Received       0
Conn Sync Update Age:            Sent       0         Received       0
Conn Sync Del Session:           Sent       0         Received       0
Conn Sync Create Persist Sess:   Sent       0         Received       0
Conn Sync Update Persist Age:    Sent       0         Received       0
Conn Sync Del Persist Session:   Sent       0         Received       0
```

```
HA errors:
Dup HA ID             0         Invalid Group        0
Version Mismatch      0         SetId Mismatch       0
Missed Heartbeat      0         Timer Msgs           0

HA Port     Sent        Recvd       Missed Heartbeat Backup Triggered Backup
Stopped
5           0           0           0                0                0
```

Table 41 describes the fields in the command output.

TABLE 41 show ha detail fields

Field	Description
Local Unit	Shows the HA operational status of this AX device: • Up – All configured HA router and server interfaces are up. • Partially Up – Some HA router or server interfaces are down but at least one server link and one router link are up. • Down – All router interfaces, or all server interfaces, or both are down. The status also is Down if both router interfaces and server interfaces are not configured and an HA interface goes down
Peer Unit	Shows the HA operational status of the other AX device. **Note:** If the status is Incompatible Version, the AX devices are running different software versions and the HA feature is not compatible between the two versions. This message is normal during upgrade, after one of the AX devices has been upgraded and before the other device is upgraded. If the devices are not being upgraded, it is recommended to upgrade one of the devices so that they both are running the same software version.
HA Group	Shows HA group information: • Unit – Indicates whether the information below is for this AX device (Local) or the other AX device (Peer). • State – Indicates whether the AX device is active or is a standby. • Priority – HA priorities configured for this group on this AX device and on its peer AX device.
Transitions	Number of times this AX device has transitioned to the active or standby state.
Connectivity	Shows the number of HA interfaces designated as server or router interfaces that are currently up.
HA packets	Shows the number of HA hello (heartbeat) packets sent or received by this AX device.
Conn Sync	Shows the number of HA connection synchronization (session mirroring) packets sent or received by this AX device.

TABLE 41 show ha detail fields (Continued)

Field	Description
Conn Query	Shows the number of HA connection query packets sent or received by this AX device.
Conn Sync Create Session	Shows the number of create session packets sent or received by this AX device.
Conn Sync Update Age	Shows the number of age update packets that were sent or received by this AX device.
Conn Sync Del Session	Shows the number of session delete packets that were sent or received by this AX device.
Conn Sync Create Persist Sess	Shows the number of create persistent session packets sent or received by this AX device.
Conn Sync Update Persist Age	Shows the number of persistent session age update packets that were sent or received by this AX device.
Conn Sync Del Persist Session	Shows the number of persistent session delete packets that were sent or received by this AX device.
HA errors	Shows HA error statistics: • Dup HA ID – Number of incoming HA hello (heartbeat) packets that had the same HA ID as the HA ID of this AX device (the local AX device). • Invalid Group – Number of incoming HA hello packets that had an invalid group ID. • Version Mismatch – Number of incoming HA hello packets that had a packet version mismatch. • SetId Mismatch – Number of incoming HA hello packets that had an HA set ID mismatch. • Missed Heartbeat – Total number of heartbeat (hello) packets expected from the peer HA device that were not received. • Timer Msgs – Number of times HA internal timers detected a variance.
HA Port	Shows statistics for each HA interface: • Sent – Number of hello (heartbeat) messages sent on the interface. • Recvd – Number of hello messages received on the interface. • Missed Heartbeat – Number of hello messages that were expected to be received on the interface but that did to arrive. • Backup Triggered – • Backup Stopped –

Example

The following command shows the HA commands in the running-config:

```
AX#show ha config
ha id 1
ha group 1 priority 255
ha group 2 priority 255
ha time-interval 3
ha preemption-enable
ha conn-mirror ip 172.22.66.2
```

show ha mac

Description

Show the virtual MAC addresses associated with HA groups.

Syntax

show ha mac

Mode

All

Usage

Each HA group has a shared MAC address, ***02***1f.a0000.00***xx***. The ***02*** portion of the address indicates this is an HA virtual MAC address, instead of a system MAC address (00). The ***xx*** portion of the address is unique to the HA group. The shared MAC address is used for all IP addresses for which HA is provided (SLB VIPs, source NAT addresses, floating IP addresses, and so on).

Example

The following command shows the virtual MAC addresses for configured HA groups 1 and 2:

```
AX#show ha mac
HA Group  MACs
1         021f.a000.0001
2         021f.a000.0021f
```

show hardware

Description

Show status information for system hardware.

Syntax

show hardware

Mode

All

Example The following command shows hardware information for an AX 2500.

```
AX2500(config)#show hardware
AX Series Advanced Traffic Manager AX2500
      Serial No : AX25061111010069
      CPU       : Intel(R) Xeon(R) CPU
                  8 cores
                  5  stepping
      Storage   : Single 74G drive
      Memory    : Total System Memory 6122 Mbyte, Free Memory 1718 Mbyte
      SMBIOS    : Build Version: 080015
                  Release Date: 02/01/2010
      SSL Cards : 1 device(s) present
                  1 Nitrox PX
      GZIP      : 0 compression device(s) present
      FPGA      : 0 instance(s) present
      L2/3 ASIC : 0 device(s) present
```

show health

Description Show status information for health monitors.

Syntax

```
show health
{
external [name] |
gateway |
monitor [name] |
postfile [name] |
stat
}
```

Parameter	Description
`external [name]`	Shows configuration settings for the specified external health monitoring program.
`gateway`	Shows configuration settings and statistics for gateway health monitoring.
`monitor [name]`	Shows configuration settings and status for the specified health monitor.
`postfile [name]`	Shows the files used for POST requests in HTTP/ HTTPS health checks.
`stat`	Shows health monitoring statistics. The statistics apply to all health monitoring activity on the AX Series device.

Mode All

Example The following command shows configuration settings and status for health monitor “ping”:

```
AX#show health monitor ping
Monitor Name:  ping
Interval:      30
Max Retry:     3
Timeout:       5
Status:        In use
Method:        ICMP
```

The output shows the method used for the monitor, and the settings for each of the parameters that are configurable for that method.

Example The following command shows the configuration settings of external health monitoring program “http.tcl”:

```
AX#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 health monitoring statistics:

```
AX#show health stat
Health monitor statistics
Total run time:                       : 2 hours 1345 seconds
```

```
Number of burst:                      : 0
max scan jiffie:                      : 326
min scan jiffie:                      : 1
average scan jiffie:                  : 1
Opened socket:                        : 1140
Open socket failed:                   : 0
Close socket:                         : 1136
Send packet:                          : 0
Send packet failed:                   : 259379
Receive packet:                       : 0
Receive packet failed                 : 0
Retry times:                          : 4270
Timeout:                              : 0
Unexpected error:                     : 0
Conn Immediate Success:               : 0
Socket closed before l7:              : 0
Socket closed without fd notify:      : 0
Get retry send:                       : 0
Get retry recv:                       : 0
Configured health-check rate (/500ms) : Auto configured
Current health-check rate (/500ms):   : 1600
Total number:                         : 8009
Status UP:                            : 8009
Status DOWN:                          : 0
Status UNKN:                          : 0
Status OTHER:                         : 0

IP address           Port  Health monitor  Status Cause(Up/Down) Retry PIN
--------------------------------------------------------------------------------
10.0.0.11            80    http            UP     11 /0  @0      0     0  /0  0
10.0.0.12            80    http            UP     10 /0  @0      0     0  /0  0
```

Table 42 describes the fields in the command output.

TABLE 42 show health stat fields

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 AX device as a traffic burst, and remedied the situation.
max scan jiffie	Used by A10 Networks Technical Support.
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.

TABLE 42 show health stat fields (Continued)

Field	Description
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.
Conn Immediate Success	Used by A10 Networks Technical Support.
Socket closed before l7	
Socket closed without fd notify	
Get retry send	
Get retry recv	
Configured health-check rate	If auto-adjust is enabled, shows “Auto configured”. If auto-adjust is disabled, shows the manually configured threshold.
Current health-check rate	If auto-adjust is enabled, shows the total number of health monitors divided by the global health-check timeout: `total-monitors / global-timeout` If auto-adjust is disabled, shows the manually configured threshold.
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 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.

TABLE 42 show health stat fields (Continued)

Field	Description
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: • ICMP – Server health check. Every 5 seconds, the AX 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 AX device. If the server does not reply after the fourth attempt (the first attempt followed by 3 retries), the AX device sets the server state to DOWN. • UDP – Protocol port health check. Every 5 seconds, the AX 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.
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. (See “show health stat Up / Down Causes” on page 799.)
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. • Current successful up-retries – Displayed to the right of the slash (/). Number of successful health check replies received for the current health check. This field is applicable if the **up-retry** option is configured for the health check. (See “health monitor” on page 128.)

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 commands entered by the tech writer while drafting this chapter:

```
AX#show history
  enable
  show version
  show access-list
  show admin
  show admin admin
  show admin detail
  show admin session
  show admin admin detail
  show arp
  show arp 192.168.1.144
  show bootimage
  show bw-list
  show clock
  show clock detail
  show core
  show cpu interval 1
  show cpu interval 10
  show debug
  show disk
  show dumpthread
--MORE--
```

show icmp

Description

Show ICMP rate limiting configuration settings and statistics.

Syntax

```
show icmp
```

Mode

All

Example

The following command shows ICMP rate limiting settings, and the number of ICMP packets dropped because the threshold has been exceeded:

```
AX(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 interfaces

Description

Display interface configuration and status information.

Syntax

```
show interfaces
[brief] |
[ethernet [port-num]] | [ve [vlan-id]] |
  [loopback num] | [management]
```

Note: For information about the **statistics** options, see “show interfaces statistics” on page 726.

Mode

Privileged EXEC level and configuration levels

Example

The following example shows brief interface information:

```
AX#show interfaces brief
Port Link  Dupl  Speed Trunk Vlan MAC             IP Address        Total IPs
-----------------------------------------------------------------------------
mgmt Up    Full  100   N/A   N/A  0090.0b0a.a594  192.168.20.241/24     1
1    Up    Full  1000  None  1    0090.0b0a.a596  10.10.10.241/24       5
2    Up    Full  1000  None  1    0090.0b0a.a597  20.20.20.241/24       1
3    Down  None  None  None  1    0090.0b0a.a598  0.0.0.0/0             0
4    Down  None  None  None  1    0090.0b0a.a599  0.0.0.0/0             0
5    Disb  None  None  None  1    0090.0b0a.a59a  0.0.0.0/0             0
6    Disb  None  None  None  1    0090.0b0a.a59b  0.0.0.0/0             0
7    Up    Full  1000  None  1    0090.0b0a.a59c  70.70.70.241/24       4
8    Disb  None  None  None  1    0090.0b0a.a59d  0.0.0.0/0             0
...
ve4  Down  N/A   N/A   N/A   4    0090.0b0a.a597  60.60.60.241/24       2
ve6  Up    N/A   N/A   N/A   5    0090.0b0a.a597  99.99.99.241/24       1
lo2  Up    N/A   N/A   N/A   N/A  N/A             68.67.65.64/23        3
```

Example

The following example shows information for Ethernet port 1:

```
AX#show interfaces ethernet 1
Ethernet 1 is up, line protocol is up
  Hardware is GigabitEthernet, Address is 0090.0b0a.a596
  Internet address is 10.10.10.241, Subnet mask is 255.255.255.0
  Internet address is 10.10.10.242, Subnet mask is 255.255.255.0
  Internet address is 10.10.10.243, Subnet mask is 255.255.255.0
  Internet address is 10.10.10.244, Subnet mask is 255.255.255.0
  Internet address is 10.10.11.244, Subnet mask is 255.255.255.0
  Configured Speed auto, Actual 1Gbit, Configured Duplex auto, Actual fdx
  Member of L2 Vlan 1, Port is Untagged
  Flow Control is enabled, IP MTU is 1500 bytes
  Port as Mirror disabled, Monitoring this Port disabled
  0 packets input,  0 bytes
  Received 0 broadcasts,  Received 0 multicasts,  Received 0 unicasts
  0 input errors,  0 CRC  0 frame
  0 runts  0 giants
  0 packets output  0 bytes
  Transmitted 0 broadcasts  0 multicasts  0 unicasts
  0 output errors  0 collisions
  300 second input rate: 158073232 bits/sec, 154368 packets/sec, 15% utiliza-
tion
  300 second output rate: 35704 bits/sec, 5 packets/sec, 0% utilization
```

Example The following example shows information for loopback interface 8:

```
AX#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
```

show interfaces statistics

Description Display interface statistics.

Syntax

```
show interfaces statistics
[ethernet portnum [ethernet portnum ...]]
[{in-pps | in-bps | out-pps | out-bps}]
[interval seconds]
```

Parameter	Description
ethernet *portnum*	Ethernet data interface numbers for which to display statistics. If you omit this option, statistics are displayed for all Ethernet data interfaces.
in-pps	Inbound traffic, in packets per second (PPS).
in-bps	Inbound traffic, in bytes per second (BPS).
out-pps	Outbound traffic, in packets per second (PPS).
out-bps	Incoming traffic, in bytes per second (BPS).
interval *seconds*	Refreshes the statistics at the specified interval, 1-32 seconds. If you do not use this option, the statistics are displayed only once.

Mode Privileged EXEC level and configuration levels

show ip

Description Show the IP mode in which the AX device is running, gateway or transparent mode.

Syntax

```
show ip
```

Mode All

Example The following command shows that the AX device is running in gateway mode:

```
AX#show ip
System is running in Gateway Mode
```

show ip bgp

Description Display information for Border Gateway Protocol (BGP). See "BGP Show Commands" on page 432.

show ip dns

Description Display the DNS configuration.

Syntax

```
show ip dns
```

show {ip | ipv6} fib

Description Display Forwarding Information Base (FIB) entries.

Note: This command is applicable only on AX Series 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 FIB entries on an AX Series device configured in route mode:

```
AX#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:

```
AX(config)#show ipv6 fib
Prefix                      Next Hop        Interface       Metric     Index
----------------------------------------------------------------------------
b101::/64                   ::              Ethernet 6      256        0
Total routes = 1
```

show {ip | ipv6} fragmentation statistics

Description Show statistics for IP fragmentation.

Syntax **`show {ip | ipv6} fragmentation statistics`**

Mode All

Example The following command shows IPv4 fragmentation statistics:

```
AX(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
Other Received                           0
ICMP Dropped                             0
ICMPv6 Dropped                           0
UDP Dropped                              0
TCP Dropped                              0
IP-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
```

Table 43 describes the fields in the command output.

TABLE 43 show {ip | ipv6} fragmentation statistics fields

Field	Description
Session Inserted	Number of times the AX device received a new fragment that did not match any existing session (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.
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.
IP-in-IP Dropped	Number of IP-in-IP fragments that were dropped.
Other Dropped	Number of other types of fragments that were dropped.

TABLE 43 show {ip | ipv6} fragmentation statistics fields (Continued)

Field	Description
Overlapping Fragment Drop	Number of fragments dropped because the data in the fragment overlapped with data in another fragment already received by the AX 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 AX device ran out of memory for fragment sessions.
Fragmentation Fast Aging Set	Number of times the AX device sped up aging of existing fragment sessions in order to accommodate new sessions.
Fragmentation Fast Aging Unset	Number of times the AX 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 AX device was exceeded.

TABLE 43 show {ip | ipv6} fragmentation statistics fields (Continued)

Field	Description
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 Reassembly Success	Number of times all fragments for a packet were 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.
IPv4-in-IPv6 Fragmentation Statistics (Not shown in the example above.)	These are the same as the counters described above, but they apply to packets fragmented into IPv4 fragments before being sent in the IPv6 tunnel. For example, these counters can apply to fragmented DS-Lite traffic. These counters are displayed if you use the **ipv6** option instead of the **ip** option.

show ip helper-address

Description Display DHCP relay information.

Syntax `show ip helper-address [detail]`

Mode All

Example The following command shows summary DHCP relay information:

```
AX(config)#show ip helper-address
Interface  Helper-Address            RX            TX      No-Relay         Drops
---------  --------------  ------------  ------------  ------------  ------------
eth1       100.100.100.1              0             0             0             0
ve5        100.100.100.1           1669          1668             0             1
ve7                                1668          1668             0             0
ve8        100.100.100.1              0             0             0             0
ve9        20.20.20.102               0             0             0             0
```

Table 44 describes the fields in the command output.

TABLE 44 show ip helper-address fields

Field	Description
Interface	AX 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: • 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:

```
AX#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
```

Table 45 describes the fields in the command output.

TABLE 45 show ip helper-address detail fields

Field	Description
IP Interface	AX interface.
Helper-Address	IP address configured on the AX 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 directly from the client to the server and do not need relay intervention.

TABLE 45 show ip helper-address detail fields (Continued)

Field	Description
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 (AX 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 | ipv6} interfaces

Description

Display IP interfaces.

```
show {ip | ipv6} interfaces
[ethernet port-num] |
[ve ve-num] |
[loopback lb-num] |
[management]
```

Mode

All

Example

The following command shows the IPv4 interfaces configured on Ethernet interface 1:

```
AX#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:

```
AX#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. (For more information, see “ip address” on page 210.)

show {ip | ipv6} isis

Description Display information for Intermediate System to Intermediate System (IS-IS) routing. See “Show Commands for IS-IS” on page 389.

show ip nat

Description Display NAT information.

Syntax **show ip nat** *option*

Option	Description
alg {http | pptp} {statistics | status}	Shows information for NAT Application Level Gateway (ALG) traffic for Hypertext Transfer Protocol (HTTP) or Point-to-Point Tunneling Protocol (PPTP). **statistics** – Shows statistics. **status** – Shows whether the feature is enabled.
interfaces	Shows the NAT direction enabled on each interface.
l4	Shows Layer 4 statistics.

logging statistics Shows statistics for NAT logging.

lsn Shows Large Scale NAT (LSN) information. See "LSN Show Commands" on page 485.

pcp statistics Shows statistics for Port Control Protocol (PCP).

pool [*pool-name*] [**statistics**] Shows pool information.

pool-group [*pool-group-name*] Shows pool group information.

range-list *range-name* Shows configured static NAT ranges.

static-binding [*ipaddr*] | [**statistics** [*ipaddr*]] Shows configuration information or statistics for static NAT bindings.

statistics Shows NAT statistics.

template Shows information for NAT templates, if configured.

timeouts Shows the timer settings.

Mode All

Example The following command shows the NAT interface settings:

```
AX#show ip nat interfaces
Total IP NAT Interfaces configured: 2
Interface       NAT Direction
-----------------------------
ve10            outside
ve11            inside
```

Example The following command shows the configured NAT pools:

```
AX#show ip nat pool
Total IP NAT Pools: 6
Pool Name    Start Address    End Address      Mask  Gateway          HA Group
-----------------------------------------------------------------------------
172.pool1    192.168.66.201   192.168.66.201    /24   0.0.0.0           1
172.pool3    192.168.66.215   192.168.66.217    /24   0.0.0.0           1
```

Example The following command shows NAT pool statistics:

```
AX#show ip nat pool statistics
Pool                 Address          Port Usage   Total Used   Total Freed
----------------------------------------------------------------------------
172.pool1            192.168.66.201   0            0            0
Pool                 Address          Port Usage   Total Used   Total Freed
----------------------------------------------------------------------------
172.pool3            192.168.66.215   0            0            0
                     192.168.66.216   0            0            0
                     192.168.66.217   0            0            0
```

In the **show ip nat pool statistics** output, the Address column lists the source addresses that are bound to NAT addresses. The Port Usage column indicates how many sessions are currently being NATted for each address. Each session counted here uses a unique TCP or UDP protocol port. ICMP traffic does not cause this counter to increment.

The Total Used column indicates the total number of sessions that have been NATted for the source address. The Total Freed column indicates how many NATted sessions have been terminated, thus freeing up a port for another session.

Example The following command displays statistics for static source NAT bindings:

```
AX#show ip nat static-binding statistics
Source Address   Port Usage   Total Used   Total Freed
------------------------------------------------------------------------------
30.30.31.35      1727         329756       328029
30.30.31.36      1799         343950       342151
30.30.31.37      1793         346257       344464
30.30.31.38      1829         232605       230776
30.30.31.39      1738         241147       240937
30.30.31.40      1774         286022       284248
```

Example The following command shows NAT statistics:

```
AX#show ip nat statistics
 Outside interfaces: ethernet1
 Inside interfaces:  ethernet3
 Hits: 1  Misses: 0
 Outbound TCP sessions created: 6
 Outbound  UDP sessions created: 7
 Outbound  ICMP sessions created: 8
 Inbound  TCP sessions created: 8
 Inbound  UDP sessions created: 2
 Dynamic mappings:
```

```
 -- Inside Source
 access-list 1 pool p2
 start 192.168.217.200 end 192.168.217.200
 total addresses 1, allocated 0, misses 0
```

Example The following command shows NAT timeout settings:

```
AX#show ip nat timeouts
NAT Timeout values in seconds:
SYN    TCP    UDP    ICMP
------------------------
60     300    300    fast
Service 53/udp has fast-aging configured
```

In this example, the output indicates that fast aging is used for IP NATted ICMP sessions, and for IP NATted DNS sessions on port 53.

The message at the bottom of the display indicates that the fast aging setting (SLB MSL timeout) will be used for IP NATted UDP sessions on port 53. If the message is not shown in the output, then the timeout shown under “UDP” will be used instead.

The following command displays PPTP NAT ALG statistics.

```
AX(config-if:ethernet2)#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 Session Drops:          4
```

Table 46 describes the fields in the command output.

TABLE 46 show ip nat alg pptp statistics fields

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 AX 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.
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 AX device.
Unknown GRE Packets	Number of GRE packets that were not used for PPTP and were dropped.
No Matching Session Drops	Number of GRE PPTP packets sent with no current call.

show ipv6 nat interfaces

Description Display a list of the IPv6 interfaces on which inside NAT or outside NAT is enabled.

Syntax

```
show ipv6 nat interfaces
```

show ipv6 ndisc

Description Display information for IPv6 router discovery.

Syntax

```
show ipv6 ndisc router-advertisement
{ethernet portnum | ve ve-num | statistics}
```

Mode All

The following command displays configuration information for IPv6 router discovery on an Ethernet interface. In this example, the interface is VE 10.

```
AX#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:

```
AX(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 AX device.

The Src Link-Layer Option and Unspecified Address counter indicates the number of times the AX 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 AX 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-addr*]

Mode All

Example The following command shows IPv6 neighbors:

```
AX(config)#show ipv6 neighbor
Total IPv6 neighbor entries: 2
IPv6 Address              MAC Address     Type      Age  State         Interface    Vlan
-------------------------------------------------------------------------------------------
b101::1112                0007.E90A.4402  Dynamic   30   Reachable     ethernet 6   1
fe80::207:e9ff:fe0a:4402  0007.E90A.4402  Dynamic   20   Reachable     ethernet 6   1
```

show {ip | ipv6} ospf

Description Display information for Open Shortest Path First (OSPF) routing. See “OSPF Show Commands” on page 348.

show {ip | ipv6} protocols

Description Show information for dynamic routing protocols.

Syntax **show** {**ip** | **ipv6**} **protocols** *protocol*

Parameter	Description
protocol	Specifies the routing protocol: **bgp** – Border Gateway Protocol (BGP). **isis** – Intermediate System to Intermediate System (IS-IS). **ospf** – Open Shortest Path First (OSPF). **rip** – Routing Information Protocol (RIP).

Mode

All

show {ip | ipv6} rip

Description

Show information for Routing Information Protocol (RIP). See “RIP Show Commands” on page 308.

show ip route

Description

Display the IPv4 routing table.

Syntax

```
show ip route
[
ipaddr[/mask-length] |
all |
connected |
database |
floating-ip |
ip-nat |
ip-nat-list |
isis |
kernel |
mgmt |
ospf |
selected-vip |
static |
summary |
vip
]
```

Mode

All

Usage

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:

```
AX#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
```

show ip-list

Description

show ipmi

Description

show ipv6 route

Description

Display the IPv6 routing table.

Syntax

```
show ipv6 route
[
ipv6-addr[/mask-length] |
connected |
database |
isis |
kernel |
mgmt |
ospf |
static |
summary |
]
```

Mode

All

show ipv6 traffic

Description Display IPv6 traffic statistics.

Syntax **show ipv6 traffic**

Mode All

Example The following command shows IPv6 traffic statistics:

```
AX#show ipv6 traffic
Traffic Type    Received        Sent
--------------------------------------
Neigh Solicit   2               0
Neigh Adverts   2               2
Echo Request    0               0
Echo Replies    5               0
Errors          0               0
```

show isis

Description Show information for Intermediate System to Intermediate System (IS-IS). (See "Show Commands for IS-IS" on page 389.)

show key-chain

Description Show configuration information for an authentication key chain.

Syntax **show key-chain key** *name* [**key** *num*]

Option	Description
name	Name of the key chain.
key *num*	Key number (1-255).

Mode Privileged EXEC and all Config levels

show lacp

Description

Show configuration information and statistics for Link Aggregation Control Protocol (LACP).

Syntax

```
show lacp sys-id
```

Syntax

```
show lacp counter [lacp-trunk-id]
```

Syntax

```
show lacp trunk
[
admin-key-list-details |
detail |
ve ve-num} |
summary |
lacp-trunk-id
]
```

Option	Description
sys-id	Shows the LACP system ID of the AX device.
lacp-trunk-id	Shows information only for the specified LACP trunk.
summary	Shows summary information.

Mode

All

Example

The following command shows LACP statistics:

```
AX-1#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:

```
AX-1#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 locale

Description Display the configured CLI locale.

Syntax **show locale**

Mode All

Example The following command shows the locale configured on an AX Series device:

```
AX#show locale
  en_US.UTF-8     English locale for the USA, encoding with UTF-8 (default)
```

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.

Syntax **show log** [**length** *num*] [**policy**]

Option	Description
length *num*	Shows the most recent log entries, up to the number of entries you specify. You can specify 1-1000000 entries.
policy	Shows the log settings. To display log entries, omit this option.

Mode All

Example The following command shows the log settings:

```
AX#show log policy
Syslog facility: local0
```

```
Flow-control: disable

Name                    Level
----------------------------
Console                 error
Buffer                  debugging
Email                   disable
Trap                    disable
Syslog                  debugging
Monitor                 debugging
```

Example The following command shows log entries.

```
AX#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 coun-
terType="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
Jan 17 11:14:07   Warning A10LB HTTP request has p-conn
Jan 17 11:13:23   Warning A10LB HTTP request has p-conn
Jan 17 11:12:47   Info    Load libraries in 0.047 secs
Jan 17 11:12:47   Notice  The session for user admin from 192.168.1.166 is
opened. Session ID is [4]
Jan 17 11:09:28   Warning A10LB HTTP request has p-conn
Jan 17 11:09:18   Warning A10LB HTTP response not beginning of header: 5a8^M
p;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp; ^M Korn shell programming
la
--MORE--
```

show lsn-lid

Description Show information for Limit IDs (LIDs) for Large Scale NAT (LSN). See “show lsn-lid” on page 504.

show lsn-rule-list

Description Show information for LSN rule lists. See “show lsn-rule-list” on page 504.

show lw-4o6

Description Display information for Lightweight 4over6.

Syntax

```
show lw-4o6 binding-table
[
files |
statistics |
tunnel-address ipv6addr [statistics]
]
```

Option	Description
files	Lists the configured Lightweight 4over6 binding tables. This includes any imported binding tables and any tables configured on the AX device.
statistics	Displays statistics.
tunnel-address *ipv6addr* [**statistics**]	Displays information for the specified tunnel address. If you use the **statistics** option, statistics for the tunnel address are shown.

Mode All

Example The following command displays general Lightweight 4over6 statistics:

```
AX(config-lw-4o6)#show lw-4o6 statistics
LW-4over6 Statistics:
----------------------------
Total Entries Configured                       7
Self-Hairpinning Drops                         0
All Hairpinning Drops                          0
No-Forward-Match ICMPv6 Sent                   0
No-Reverse-Match ICMP Sent                     0
Inbound ICMP Drops                             0
Forward Route Lookup Failed                    0
Reverse Route Lookup Failed                    0
```

Table 47 describes the fields in this command’s output.

TABLE 47 show lw-4o6 statistics fields

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*.
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 binding-table entry. • The destination IP address matches the IPv4 NAT address of any binding-table entry.
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 AX device receives a packet whose IPv6 tunnel address does not match any binding-table entries.
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.
Inbound ICMP Drops	Number of inbound IPv4 ICMP packets that were dropped.
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.
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.

show mac-address-table

Description

Display MAC table entries.

Syntax

```
show mac-address-table
[macaddr | port port-num | vlan vlan-id]
```

Option	Description
macaddr	Shows the MAC table entry for the specified MAC address. Enter the MAC address in the following format: aaaa.bbbb.cccc
port *port-num*	Shows the MAC table entries for the specified Ethernet port.
vlan *vlan-id*	Shows the MAC table entries for the specified VLAN.

Mode

All

Example

The following command displays the MAC table entry for MAC address 0013.72E3.C773:

```
AX#show mac-address-table 0013.72E3.C773
Total active entries: 1          Age time: 300 secs
MAC-Address       Port      Type      Index      Vlan   Age
---------------------------------------------------------
0013.72E3.C773    1         Dynamic   16         10     90
```

Table 48 describes the fields in the command output.

TABLE 48 show mac-address-table fields

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.
Age	Number of seconds since the entry was last used.

show management

Description

Show the types of management access allowed on each of the AX Series device’s Ethernet interfaces.

Syntax

`show management`

Mode

All

Usage

To configure the management access settings, see “enable-management” on page 121 and “disable-management” on page 115.

Example

The following command shows the management access settings on an AX Series device.

```
AX#show management
     PING   SSH    Telnet HTTP   HTTPS  SNMP   ACL
---------------------------------------------------------
mgmt on     on     off    on     on     on     -
1    on     off    off    off    off    off    -
2    on     off    on     off    off    off    -
3    on     off    on     off    off    off    -
4    on     off    on     off    off    off    -
5    on     off    on     off    off    off    -
6    on     off    on     off    off    off    -
7    on     off    on     off    off    off    -
9    on     off    on     off    off    off    -
10   on     off    on     off    off    off    3
ve1  on     off    on     on     off    off    -
ve2  on     off    on     off    off    off    -
```

show memory

Description

Display memory usage information.

Syntax

`show memory [cache | system]`

Option	Description
cache	Shows cache statistics.
system	Shows summary statistics for memory usage.

Mode

Privileged EXEC level and configuration levels

Example The following command shows summary statistics for memory usage:

```
AX#show memory system
System Memory Usage:
Total(KB)  Free       Shared     Buffers    Cached     Usage
---------------------------------------------------------------------------
2070368    751580     0          269560     96756      59.0%
```

show mirror

Description Display port mirroring information.

Syntax `show mirror`

Mode All

Example The following example shows the port mirroring configuration on an AX Series device:

```
AX#show mirror
Mirror Port :   4
 Port monitored at ingress : 2
 Port monitored at egress : 2
```

Table 49 describes the fields in the command output.

TABLE 49 show mirror fields

Field	Description
Mirror Port	Port to which the traffic is copied. This is the port to which the protocol analyzer should be attached.
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 The following commands set the event threshold for data CPU utilization to 80% and verify the result:

```
AX(config)#monitor data-cpu 80
AX(config)#show monitor
Current system monitoring threshold:
Hard disk usage:      85
Memory usage:         95
Control CPU usage:    90
Data CPU usage:       80
IO Buffer usage:      60000
Buffer Drop:          100
Warning Temperature:  68
```

show nat46-stateless

Description Show information for stateless NAT46. See “show nat46-stateless statistics” on page 581.

show nat64

Description Show information for NAT64. See “DNS64 / NAT64 Show Commands” on page 539.

show netflow

Description Display NetFlow information.

Syntax **show netflow monitor** [*monitor-name*]

Option	Description
monitor-name	Name of a configured NetFlow monitor.

Introduced in Release 2.6.6-P4

Mode All

show ntp

Description Show the Network Time Protocol (NTP) configuration and status.

Syntax

```
show ntp {servers | status}
```

Option	Description
`servers`	Shows the NTP configuration and shows whether the AX Series device is synchronized with the NTP server.
`status`	Shows whether the AX Series device is synchronized with the NTP server.

Mode Privileged EXEC level and configuration levels

Example The following command shows the NTP configuration and the synchronization status:

```
AX#show ntp servers

Ntp Server                              Mode
-----------------------------------------
*10.1.4.20                           enabled
```

Table 50 describes the fields in the command output.

TABLE 50 show ntp fields

Field	Description
NTP server	IP address of the NTP server.
Mode	Indicates whether NTP is enabled.

Example The following command shows the NTP synchronization status:

```
AX#show ntp status
NTP sync status: success
```

show process

Description Display the status of system processes.

Syntax **`show process system`**

Mode Privileged EXEC level and configuration levels

Usage For descriptions of the system processes, see the “AX Software Processes” section in the “System Overview” chapter of the *AX Series System Configuration and Administration Guide*.

Example The following command shows the status of system processes on an AX Series device:

```
AX#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 RADIUS statistics.

Syntax **`show radius-server`**

Mode All

show reboot

Description Display scheduled system reboots.

Syntax

```
show reboot
```

Mode All

Example The following command shows a scheduled reboot on an AX Series device:

```
AX#show reboot
Reboot scheduled for 04:20:00 PST Sun Apr 20 2008 (in 63 hours and 16 minutes)
by admin on 192.168.1.144
Reboot reason: Outlook_upgrade
```

show router log file

Description Show router logs.

Syntax

```
show router log file
[
file-num |
isisd [file-num] |
nsm [file-num] |
ospf6d [file-num] |
ospfd [file-num]
]
```

Parameter	Description
file-num	Log file number.
nsm [*file-num*]	Displays the specified Network Services Module (NSM) log file, or all NSM log files.
ospf6d [*file-num*]	Displays the specified IPv6 OSPFv3 log file, or all OSPFv3 log files.
ospfd [*file-num*]	Displays the specified IPv4 OSPFv2 log file, or all OSPFv2 log files.

Mode Any

show running-config

Description Display the running-config.

Syntax

```
show running-config
[
ha |
health-monitor [name] |
interfaces [ethernet [portnum] | ve [num] |
  loopback [num] | management |
slb [server [name] | service-group [name] |
  virtual-server [name]] |
vlan [vlan-id]
]
```

Option	Description
ha	Shows High Availability configuration commands in the running-config.
health-monitor [*name*]	Shows health-monitor configuration commands in the running-config.
slb [**server** [*name*] | **service-group** [*name*] | **virtual-server** [*name*]]	Shows SLB server, service-group, and virtual-server configuration commands in the running-config.
vlan [*vlan-id*]	Shows VLAN configuration commands in the running-config.

Mode All

Example The following command shows the running-config on an AX Series device:

```
AX#show running-config
!Current configuration : 10577 bytes
!Configuration last updated at 18:01:01 PST Mon Jan 21 2008
!Configuration last saved at 15:09:41 PST Mon Jan 21 2008
!version 2.6.1, build 169 (Jan-24-2011,12:30)
!
hostname AX2K-B
!
clock timezone America/Tijuana
!
```

```
!
!
vlan 10
 untagged ethernet 1
 router-interface ve 10
!
vlan 11
 untagged ethernet 2
 router-interface ve 11
!
vlan 20
 tagged ethernet 4
 router-interface ve 20
--MORE--
```

show session

Description

Display session information.

```
show session
[
6rd-nat64 [sub-options] |
brief |
ds-lite [sub-options] |
filter {filter-name | config} |
full-width |
ipv4 [sub-options] |
ipv6 [sub-options] |
nat44 [sub-options] |
nat64 [sub-options]
]
```

Parameter	Description
6rd-nat64 [*sub-options*]	Displays IPv6-in-IPv4 6rd-NAT64 sessions. The following *sub-options* are supported: **source-v4-addr** *ipv4addr*[/*mask-length*] – Source IPv4 address of the session. **source-v6-addr** *ipv6addr*[/*prefix*] – Source IPv6 address of the session. **source-port** *portnum* – Source protocol port of the session. **dest-v4-addr** *ipv4addr*[/*mask-length*] – Destination IPv4 address of the session. **dest-v6-addr** *ipv6addr*[/*prefix*] – Destination IPv6 address of the session. **dest-port** *portnum* – Destination protocol port of the session.
brief	Displays summary statistics for all session types.
ds-lite [*sub-options*]	Displays IPv4-in-IPv6 DS-Lite sessions. The *sub-options* are the same as those for **6rd-nat64**.

filter *filter-name* | **config**

Displays information about configured session filters.

filter-name – Displays the specified session filter.

config – Displays all configured session filters.

full-width

Displays complete IPv6 addresses instead of truncating them. (See “Usage” below.)

ipv4 [*sub-options*]

Displays IPv4 LSN sessions, IPv4 Fixed-NAT sessions, and IPv4 static mapping sessions. The following *sub-options* are supported:

source-v4-addr *ipv4addr*[*/mask-length*] – Source IPv4 address of the session.

source-port *portnum* – Source protocol port of the session.

dest-v4-addr *ipv4addr*[*/mask-length*] – Destination IPv4 address of the session.

dest-port *portnum* – Destination protocol port of the session.

ipv6 [*sub-options*]

Displays NAT64 sessions and NAT64 Fixed-NAT sessions. The following *sub-options* are supported:

source-v6-addr *ipv6addr*[*/prefix*] – Source IPv6 address of the session.

source-port *portnum* – Source protocol port of the session.

dest-v6-addr *ipv6addr*[*/prefix*] – Destination IPv6 address of the session.

dest-port *portnum* – Destination protocol port of the session.

nat44 [*sub-options*]

Displays IPv4 LSN sessions and IPv4 Fixed-NAT sessions. The *sub-options* are the same as those for **ipv4**.

nat64 [*sub-options*]

Displays NAT64 sessions and NAT64 Fixed-NAT sessions. The *sub-options* are the same as those for **ipv6**.

Mode

All

Usage

For convenience, you can save session display options as a session filter. (See “session-filter” on page 168.)

Abbreviated IPv6 Address Display

In **show session** output, IPv6 addresses are truncated by default, to a maximum of 22 characters. The truncation aligns the IPv6 output with the IPv4 output.

If you want to display the full IPv6 addresses, use the following command:
show session full-width

Notes on full-width Option

- DS-Lite addresses, which have IPv4 addresses within IPv6 tunnel addresses, are nearly always truncated. Truncated DS-Lite IPv6 addresses are shown without their IPv4 suffixes.
  Example: `[14::6 :52485`
- If the entire IPv6 address plus its protocol port ***can not*** be displayed in the space provided, the truncated IPv6 address is shown within a left bracket only. Generally, this applies to DS-Lite addresses. For example:
  `[3001::2 :37191`
- For IPv6 addresses other than DS-Lite addresses, if the entire IPv6 address plus its protocol port can be displayed within 22 spaces, the IPv6 address is shown within a pair of left and right brackets. Up to 14 spaces are allowed for the IPv6 address. Five additional spaces are used for the protocol port number. The final 3 spaces are used for the brackets and the colon in front of the port number.
  Example: `[3001::2]:16967`

Note on Clearing Sessions

After entering the **clear session** command, the AX 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

Here is an example of **show session** output containing truncated IPv6 addresses. In this example and the next one, the first address row is for DS-Lite.

```
AX#show session
Traffic Type                       Total
--------------------------------------------
TCP Established                    0
TCP Half Open                      0
..

Prot Forward Source         Forward Dest          Reverse Source        Reverse Dest          Age
Hash Flags
--------------------------------------------------------------------------------------------------
--------------
Icmp [3001::2 :37191       [3001::1 :0           30.30.30.3:0          5.5.5.71:37191        0
1    NS
Icmp [3001::2]:16967       [64:ff9b::1e1e :0     30.30.30.3:0          5.5.5.72:32768        0
1    NS
Total Sessions:          2
```

Example

The following command displays the IPv6 addresses without truncating them:

```
AX#show session full-width
Traffic Type                       Total
--------------------------------------------
TCP Established                    0
TCP Half Open                      0
...
Prot Forward Source         Forward Dest          Reverse Source        Reverse Dest          Age
Hash Flags
--------------------------------------------------------------------------------------------------
--------------
Icmp [3001::2]10.10.10.2:37191 [3001::1]30.30.30.3:0  30.30.30.3:0          5.5.5.71:37191
0     1    NS
Icmp [3001::2]:16967       [64:ff9b::1e1e:1e03]:0 30.30.30.3:0         5.5.5.72:32768        0
1    NS
Total Sessions:          2
```

Table 51 describes the fields in the command output.

TABLE 51 show session fields

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 AX Series device has not yet received a SYN ACK from the backend server.
UDP	Number of UDP sessions.
Non TCP/UDP IP sessions	Number of IP sessions other than TCP or UDP sessions. This counter applies specifically to IP protocol load balancing. (See the “IP Protocol Load Balancing” chapter in the *AX Series Application Delivery and Server Load Balancing Guide*.)
Other	Number of internally used sessions. As an example, internal sessions are used to hold fragmentation information.

TABLE 51 show session fields (Continued)

Field	Description
Reverse NAT TCP	Number of reverse-NAT TCP sessions.
Reverse NAT UDP	Number of reverse-NAT UDP sessions.
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.
Conn SMP Alloc	Statistics used by A10 Technical Support.
Conn SMP Free	
Conn SMP Aged	
Conn Type 0 Available	
Conn Type 1 Available	
Conn Type 2 Available	
Conn Type 3 Available	
Conn SMP Type 0 Available	
Conn SMP Type 1 Available	
Conn SMP Type 2 Available	
Conn SMP Type 3 Available	
The following columns list information for individual sessions.	
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, 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.

TABLE 51 show session fields (Continued)

Field	Description
Reverse Source	Real server's IP address. **Note:** If the AX device is functioning as a cache server (RAM caching), asterisks (*) in this field and the Reverse Dest field indicate that the AX device directly served the requested content to the client from the AX RAM cache. In this case, the session is actually between the client and the AX 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 AX device when connecting to the real server. • If source IP NAT *is not* used for the virtual port, this address is the client IP address.
Age	Number of seconds since the session started.
Hash	CPU ID.
Flags	Processing path for the traffic: • NF – Fast-path processing. • NS – Slow-path processing.

show sflow

Description Show sFlow configuration or statistics information.

Syntax

```
show sflow {configuration | statistics}
[ethernet port-num]
```

Introduced in Release 2.6.6-P4

Mode Privileged EXEC level and configuration levels

Example The following command shows sFlow statistics on an AX Series device:

```
AX(config)#show sflow statistics
Interface      Packet Sample Records      Counter Sample Records
------------------------------------------------------------------
------------------------------------------------------------------
sFlow total statistics
   Packet sample records:          9
   Counter sample records:         10
   sFlow packets sent:             1
```

Example The following command shows sFlow configuration, including status of the cpu-usage and lsn-pool-usage, on an AX Series device:

```
AX(config)#show sflow configuration
sFlow collector not set,sFlow is disabled
sFlow agent
   address:                        not set, use management ip address
sFlow default parameter
   counter polling interval:       20
   packet sampling rate:           1000
sflow polling cpu-usage
sflow polling lsn-pool-usage
```

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 AX Series device:

```
AX#show shutdown
Shutdown scheduled for 12:00:00 PST Sat Jan 19 2008 (in 358 hours and 23 min-
utes) by admin on 192.168.1.144
Shutdown reason: Scheduled shutdown
```

show slb l4

Description Show Layer-4 SLB statistics.

Syntax `show slb l4 [detail]`

Option	Description
`detail`	Lists separate counters for each CPU.

Mode All

Example The following command shows summary statistics for Layer 4 SLB:

```
AX#show slb l4
                         Total
------------------------------------------------------------------
IP out noroute           0
TCP out RST              0
TCP out RST no SYN       0
TCP out RST L4 proxy     0
TCP out RST ACK attack   0
TCP out RST aFleX        0
TCP out RST stale sess   2
TCP out RST TCP proxy    1906748
TCP SYN received         17556
TCP SYN cookie snt       3276
TCP SYN cookie snt fail  0
TCP received             2014764
UDP received             0
Server sel failure       0
Source NAT failure       0
Source NAT no fwd route  0
Source NAT no rev route  0
Source NAT ICMP Process  0
Source NAT ICMP No Match 0
TCP SYN cookie failed    18
NAT no session drops     0
No SYN pkt drops         0
No SYN pkt drops - FIN   0
No SYN pkt drops - RST   0
No SYN pkt drops - ACK   0
Conn Limit drops         0
Conn Limit resets        0
Conn rate limit drops    0
Conn rate limit resets   0
Proxy no sock drops      0
aFleX drops              0
Session aged out         0
TCP Session aged out     0
UDP Session aged out     0
Other Session aged out   0
TCP no SLB               0
UDP no SLB               0
SYN Throttle             0
Inband HM retry          0
Inband HM reassign       0
Fast aging set           0
Fast aging reset         0
TCP invalid drop         0
SYN stale sess drop      0
Anomaly out of sequence  0
Anomaly zero window      0
Anomaly bad content      0
Anomaly pbslb drop       0
No resource drop         0
Reset unknown conn       0
ignore msl               0
```

Table 52 describes the fields in the command output.

TABLE 52 show slb l4 fields

Field	Description
IP out noroute	Number of IP packets that could not be routed.
TCP out RST	Number of TCP Resets sent.
TCP out RST no SYN	Number of Resets sent for which there was no SYN.
TCP out RST L4 proxy	Number of TCP Reset packets the AX device has sent as a Layer 4 proxy.
TCP out RST ACK attack	Number of TCP Resets sent in response to a TCP ACK attack.
TCP out RST aFleX	Number of TCP Reset packets the AX device has sent due to an aFleX policy. (Not applicable to IPv6 migration releases.)
TCP out RST stale sess	Number of TCP Reset packets the AX device has sent due to stale TCP sessions.
TCP out RST TCP proxy	Number of TCP Reset packets the AX device has sent as a TCP proxy.
TCP SYN received	Number of TCP SYN packets received.
TCP SYN cookie snt	Number of TCP SYN cookies sent.
TCP SYN cookie snt fail	Number of TCP SYN cookie send attempts that failed.
TCP received	Number of TCP packets received.
UDP received	Number of UDP packets received.
Server sel failure	Number of times selection of a real server failed.
Source NAT failure	Number of times a source NAT failure occurred.
Source NAT no fwd route	Number of times there was no route to the destination for Layer 3 NAT traffic.
Source NAT no rev route	Number of times there was no route to the source for Layer 3 NAT traffic.
Source NAT ICMP Process	Number of times an ICMP error related to source NAT occurred.
Source NAT ICMP No Match	Number of times an ICMP error related to source NAT occurred, and there was no matching session for the traffic.
TCP SYN cookie failed	Number of times a TCP SYN cookie failure occurred.
NAT no session drops	Number of times non-ICMP traffic to a NAT IP address was dropped because there was no matching session.
No SYN pkt drops	Number of SYN packets dropped.
No SYN pkt drops - FIN	Number of SYN packets dropped due to a TCP FIN.

TABLE 52 show slb l4 fields (Continued)

Field	Description
No SYN pkt drops - RST	Number of SYN packets dropped due to a TCP Reset.
No SYN pkt drops - ACK	Number of SYN packets dropped due to an ACK.
Conn Limit drops	Number of connections dropped because the server connection limit had been reached.
Conn Limit resets	Number of connections reset because the server connection limit had been reached.
Conn rate limit drops	Number of connections dropped by connection rate limiting.
Conn rate limit resets	Number of connections reset by connection rate limiting.
Proxy no sock drops	Number of packets dropped because the proxy did not have an available socket.
aFleX drops	Number of packets dropped due to an aFleX policy. (Not applicable to IPv6 migration releases.)
Session aged out	Total number of sessions that have aged out.
TCP Session aged out	Number of TCP sessions that have aged out.
UDP Session aged out	Number of UDP sessions that have aged out.
Other Session aged out	Number of sessions of other types (not TCP or UDP) that have aged out.
TCP no SLB	Number of non-SLB TCP packets received by the AX device.
UDP no SLB	Number of non-SLB UDP packets received by the AX device.
SYN Throttle	Number of SYN packets that have been throttled.
Inband HM retry	Number of times the AX device retried an inband health check, because a SYN-ACK was not received for the previous SYN.
Inband HM reassign	Number of times the AX device reassigned a client's traffic to another server, because the initial server exceeded the maximum number of retries allowed by the inband health check.
Fast aging set	Please contact A10 Networks for information.
Fast aging reset	Please contact A10 Networks for information.
TCP invalid drop	Please contact A10 Networks for information.
SYN stale sess drop	Please contact A10 Networks for information.
Anomaly out of sequence	Number of packets that matched an IP anomaly out-of-sequence filter. **Note:** To configure IP anomaly filters, see "ip anomaly-drop" on page 239.

TABLE 52 show slb l4 fields (Continued)

Field	Description
Anomaly zero window	Number of packets that matched an IP anomaly zero-window filter.
Anomaly bad content	Number of packets that matched an IP anomaly bad-content filter.
Anomaly pbslb drop	Number of packets that matched an IP anomaly filter used for system-wide Policy-Based SLB (PBSLB).
No resource drop	Please contact A10 Networks for information.
Reset unknown conn	Please contact A10 Networks for information.
ignore msl	Number of packets dropped by the ignore-tcp-msl option. (See "slb template virtual-port" on page 637.)

show slb performance

Description Show SLB performance statistics.

Syntax

```
show slb performance
[interval number [detail]]
[{l4cpi | l7cpi | l7tpi | natcpi | sslcpi}
  [detail]]
```

Option	Description
interval *number*	Automatically refreshes the output at the specified interval. The interval can be 1-32 seconds. If you omit this option, the output is shown one time. If you use this option, the output is repeatedly refreshed at the specified interval until you press ctrl+c.
detail	Lists separate counters for each CPU.
l4cpi	Shows only Layer 4 connections per interval.
l7cpi	Shows only Layer 7 connections per interval.
l7tpi	Shows only Layer 7 transactions per interval.
natcpi	Shows only Network Address Translation (NAT) connections per interval.
sslcpi	Shows only SSL connections per interval.
detail	This option is not used in the current release.

Mode All

Example The following command shows SLB performance statistics:

```
AX#show slb performance
Refreshing SLB performance every 1 seconds. (press ^C to quit)
Note: cpi conn/interval, tpi transactions/interval

CPU Usage    L4cpi      L7cpi      L7tpi      SSLcpi     Natcpi     Time
-----------------------------------------------------------------------
8/9          0          0          0          0          0          11:46:10
4/4          4222       0          0          0          0          11:46:11
4/4          3          0          0          0          0          11:46:12
```

Table 53 describes the fields in the command output.

TABLE 53 show slb performance fields

Field	Description
Refreshing SLB performance every # seconds	Interval at which the statistics are refreshed.
CPU Usage	Utilization on each data CPU. Each number is the utilization on one data CPU. In the example shown above, the AX model has three data CPUs, and the utilization on each one is 1%.
L4cpi	Layer 4 connections per interval.
L7cpi	Layer 7 connections per interval.
L7tpi	Layer 7 transactions per interval.
SSLcpi	SSL connections per interval.
Natcpi	NAT connections per interval.
Time	System time when the statistics were collected.

show slb server

Description Show server information.

Syntax

```
show slb server
[[server-name [port-num] detail] config]
```

Option	Description
server-name [[*port-num*] **detail**]	Shows information only for the specified server or port. If you omit this option, information is shown for all real servers and ports. The **detail** option shows statistics for the specified server or port. This option also displays the name of the server or port template bound to the server or port.
config	Shows the SLB configuration of the real servers.

Mode All

show slb service-group

Description Show service-group (server pool) information.

Syntax

```
show slb service-group [group-name] [config]
```

Option	Description
group-name	Shows information only for the specified service group. If you omit this option, information is shown for all service groups configured on the AX Series device.
config	Shows the SLB configuration of the service groups.

Mode All

show slb switch

Description Show SLB switching statistics.

Syntax

```
show slb switch
[detail | ethernet port-num [detail]]
```

Option	Description
detail	Shows detailed statistics.
ethernet *port-num*	Shows statistics only for the specified Ethernet port.

Mode All

Example The following command shows summary SLB switching statistics:

```
AX#show slb switch
                         Total
------------------------------------------------------------------
L2 Forward               0
L3 IP Forward            0
IPv4 No Route Drop       0
L3 IPv6 Forward          0
IPv6 No Route Drop       0
L4 Process               0
Incorrect Len Drop       0
Prot Down Drop           0
Unknown Prot Drop        0
TTL Exceeded Drop        0
Link Down Drop           0
SRC Port Suppression     0
L2 Default Vlan FWD Drop 0
MAX ARP Drop             0
VLAN Flood               0
IP Fragment Rcvd         0
ARP REQ Rcvd             0
ARP RESP Rcvd            0
Forward Kernel           0
IP(TCP) Fragment Rcvd    0
IP Fragment Overlap      0
IP Frag Overload Drops   0
IP Fragment Reasm OKs    0
IP Fragment Reasm Fails  0
IP Fragment Timeout      0
IP Invalid Length Frag   0
Anomaly Land Attack Drop 0
Anomaly IP OPT Drops     0
Anomaly PingDeath Drop   0
Anomaly All Frag Drop    0
Anomaly TCP noFlag Drop  0
Anomaly SYN Frag Drop    0
Anomaly TCP SYNFIN Drop  0
Anomaly Any Drops        0
BPDUs Received           0
BPDUs Sent               0
ACL Denys                0
```

```
SYN rate exceeded Drop   0
Packet Error Drops       0
IPv6 Frag Reasm OKs      0
IPv6 Frag Reasm Fails    0
IPv6 Frag Invalid Pkts   0
Bad Pkt Drop             0
IP Frag Exceed Drop      0
IPv4 No L3 VLAN FWD Drop 0
IPv6 No L3 VLAN FWD Drop 0
L2 Default Vlan FWD Drop 0
BW Limit Drop            0
License Expire Drop      0
IPV6 DAD on Solicits     0
IPV6 DAD on Adverts      0
IPV6 DAD MAC conflicts   0
IPV6 DAD Out-of-memory   0
```

Table 54 describes the fields in the command output.

TABLE 54 show slb switch fields

Field	Description
L2 Forward	Number of packets that have been Layer 2 switched.
L3 IP Forward	Number of packets that have been Layer 3 routed.
IPv4 No Route Drop	Number of IPv4 packets that were dropped due to routing failures.
L3 IPv6 Forward	Number of IPv6 packets that have been Layer 3 routed.
IPv6 No Route Drop	Number of IPv6 packets that were dropped due to routing failures.
L4 Process	Number of packets that went to a VIP or NAT for processing.
Incorrect Len Drop	Number of packets dropped due to incorrect protocol length. **Note:** A high value for this counter can indicate a packet length attack.
Prot Down Drop	Number of packets dropped because the corresponding protocol was disabled.
Unknown Prot Drop	Number of packets dropped because the protocol was unknown.
TTL Exceeded Drop	Number of packets dropped due to TTL expiration.
Link Down Drop	Number of packets dropped because the outgoing link was down.
SRC Port Suppression	Packet drops because of source port suppression.
L2 Default VLAN FWD Drop	Please contact A10 Networks for information.
MAX ARP Drop	Please contact A10 Networks for information.
VLAN Flood	Number of packets that have been broadcast to a VLAN.

TABLE 54 show slb switch fields (Continued)

Field	Description
IP Fragment Rcvd	Number of IPv4 fragments that have been received.
ARP REQ Rcvd	Number of ARP requests that have been received.
ARP RESP Rcvd	Number of ARP responses that have been received.
Forward Kernel	Number of packets received by the kernel from data interfaces.
IP(TCP) Fragment Rcvd	Number of IP TCP fragments received.
IP Fragment Overlap	Number of overlapping fragments received.
IP Frag Overload Drops	Number of fragments dropped due to overload.
IP Fragment Reasm OKs	Number of successfully reassembled IP fragments.
IP Fragment Reasm Fails	Number of IP fragment reassembly failures.
IP Invalid Length Frag	Please contact A10 Networks for information.
IP Fragment Timeout	Please contact A10 Networks for information.
Anomaly Land Attack Drop	Number of SYN packets dropped because they were spoofed (used the destination IP address as the source IP address).
Anomaly IP OPT Drops	Number of packets dropped because they had IP options set.
Anomaly Ping-Death Drop	Number of oversized (longer than 32 K) ICMP packets dropped. An oversized ICMP packet can trigger Denial of Service (DoS), crashing, freezing, or rebooting.
Anomaly All Frag Drop	Number of IP fragments dropped.
Anomaly TCP noFlag Drop	Number of TCP packets dropped because they had no flags set. TCP packets are normally sent with at least one bit in the flags field set.
Anomaly SYN Frag Drop	Number TCP SYN fragments dropped that had the fragmentation bit set. A SYN fragment attack floods the target host with SYN packet fragments. An unprotected host will store the fragments, in order to reassemble them. By not completing the connection, and flooding the server or host with such fragmented SYN packets, the attacker can cause the host’s memory buffer to fill up eventually.

TABLE 54 show slb switch fields (Continued)

Field	Description
Anomaly TCP SYNFIN Drop	Number of TCP packets dropped that had TCP SYN *and* FIN bits set. An attacker can send a packet with both bits set to determine what kind of system reply is returned, and then use the system information for further attacks using known system vulnerabilities. Also, some older devices will let such packets through even though there is an established ACL defined and the state of the TCP connection is not considered to be established.
Anomaly Any Drops	Total number of packets dropped by IP anomaly filtering.
BPDUs Received	Number of Bridge Protocol Data Units (BPDUs) received.
BPDUs Sent	Number of Bridge Protocol Data Units (BPDUs) sent.
ACL Denys	Number of times traffic was not forwarded due to a deny rule in an Access Control List (ACL). This counter also includes traffic dropped due to the l3-vlan-fwd-disable action in ACL rules.
SYN rate exceeded Drop	Number of packets dropped because the TCP SYN threshold had been exceeded.
Packet Error Drops	Number of packets dropped due to a packet error.
IPv6 Frag Reasm OKs	Number of successfully reassembled IPv6 fragments.
IPv6 Frag Reasm Fails	Number of IPv6 fragment reassembly failures.
IPv6 Frag Invalid Pkts	Number of IPv6 fragments that were invalid.
Bad Pkt Drop	Number of bad packets dropped.
IP Frag Exceed Drop	Number of fragmented IP packets that were dropped because they exceeded the allowed maximum.
IPv4 No L3 VLAN FWD Drop	Number of IP packets that were dropped by the l3-vlan-fwd-disable action in an IPv4 ACL.
IPv6 No L3 VLAN FWD Drop	Number of IP packets that were dropped by the l3-vlan-fwd-disable action in an IPv6 ACL.
L2 Default VLAN FWD Drop	Please contact A10 Networks for information.
BW Limit Drop	Number of packets dropped because they exceeded the bandwidth limit. **Note:** This field applies only to the SoftAX.
License Expire Drop	Number of packets dropped due to an invalid license. **Note:** This field applies only to the SoftAX.

TABLE 54 show slb switch fields (Continued)

Field	Description
IPv6 DAD on Solicits	Number of duplicate address detections due to a neighbor tried to configure or use an IPv6 address that was already in use on the AX device.
IPv6 DAD on Adverts	Number of duplicate address detections that occurred because an AX admin attempted to configure an IPv6 address that was already in use by a neighbor.
IPv6 DAD MAC Conflicts	Number of neighbors that triggered DAD with the AX device, or with which the AX device triggered DAD.
IPv6 DAD Out-of-memory	Number of times there were more than 512 DAD events during a 10-second interval. The AX device logs each DAD event in the log, and can log up to 512 events per 10-second interval.

show slb template

Description

Show template configuration information.

Syntax

```
show slb template [{dns | policy} template-name]
```

Mode

All

show slb virtual-server

Description

Show virtual-server information.

Default

```
show slb virtual-server
[
virtual-server-name
   [[virtual-port-num service-type
      [service-group-name]]
    detail]
[bind]
[config]
```

Option	Description
virtual-server-name	Shows information only for the specified virtual server. The *virtual-port-num service-type* option shows information only for the specified virtual port on the virtual server.

	The *service-group-name* option further restricts the output, to show information only for the specified service group. The **detail** option displays connection and packet statistics.
`bind`	Includes the service groups and real servers and ports bound to the virtual ports.
`config`	Displays virtual-server configuration information.

Mode All

show smtp

Description Display SMTP information.

Syntax

```
show smtp
```

Mode All

Example The following command show the SMTP server address:

```
AX#show smtp
SMTP server address:         192.168.1.99
```

show startup-config

Description Display a configuration profile or display a list of all the locally saved configuration profiles.

Syntax

```
show startup-config
[
all [cf] |
profile profile-name [cf]
]
```

Mode All

Option	Description
`all [cf]`	Displays a list of the locally stored configuration profiles. The **cf** option displays all the configuration profiles stored on the compact flash.

profile *profile-name* [*options*]

Displays the commands that are in the specified configuration profile.

The **cf** option displays the configuration profile on the compact flash rather than the hard disk. If you omit this option, the configuration profile on the hard disk is displayed.

The **all-partitions** option shows all resources in all partitions.

The **partitions** option shows only the resources in the specified partition.

Mode

All

Usage

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 AX device most recently rebooted.

Example

The following command shows the configuration profile currently linked to startup-config on an AX Series device:

```
AX#show startup-config
Building configuration...

!Current configuration: 10580 bytes
!Configuration last updated at 15:01:01 PST Mon Jan 21 2008
!Configuration last saved at 15:09:41 PST Mon Jan 21 2008
!version 2.6.1, build 169 (Jan-24-2011,12:30)
!
hostname AX2K-B
!
clock timezone America/Tijuana
!
!
!
vlan 10
 untagged ethernet 1
 router-interface ve 10
!
vlan 11
 untagged ethernet 2
 router-interface ve 11
!
vlan 20
--MORE--
```

Example

The following command shows a list of the configuration profiles locally saved on the AX device. The first line of output lists the configuration profile that is currently linked to “startup-config”. If the profile name is “default”, then “startup-config” is linked to the configuration profile stored in the image area from which the AX device most recently rebooted.

```
AX#show startup-config all
Current Startup-config Profile: default
Profile-Name                               Size    Time
------------------------------------------------------------
1210test                                   1957    Jan 28  18:39
lb-v6                                     13414    Jan 23  19:19
```

show statistics

Description

Display packet statistics for Ethernet interfaces.

Syntax

show statistics [**interface ethernet** *port-num*]

Mode

All

Example

The following command shows brief statistics for all Ethernet interfaces on an AX Series device:

```
AX#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
...

XAUI  3171070        3118342        275613         216063         0
```

Note: The XAUI port is an internal port, not a user-configured interface.

Example

The following command shows detailed statistics for Ethernet interface 1:

```
AX#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 system platform

Description

Display platform-related information and statistics.

Syntax

```
show system platform
{
statistics |
interface-stats |
buffer-stats |
busy-counter |
drop-counter |
register-info
}
```

Option	Description
statistics	Shows counters for internal statistics.
interface-stats	Shows counters for interface statistics.
buffer-stats	Shows counters for buffer statistics.
busy-counter	Shows counters for system busy statistics.
drop-counter	Shows counters for drop statistics.
register-info	Shows register information.

Mode

All

Example

The following command shows platform buffer statistics:

```
AX#show system platform buffer-stats
# buffers in Q0 cache: 2049 App: 0 TCPQ: 0 misc: 0
# buffers in Q1 cache: 4096 App: 0 TCPQ: 0 misc: 0
# buffers in Q2 cache: 4096 App: 0 TCPQ: 0 misc: 0
# buffers in Q3 cache: 4096 App: 0 TCPQ: 0 misc: 0
# buffers in Q4 cache: 4096 App: 0 TCPQ: 0 misc: 0
# buffers in Q5 cache: 4096 App: 0 TCPQ: 0 misc: 0
# buffers in Q6 cache: 4096 App: 0 TCPQ: 0 misc: 0
# buffers in Q7 cache: 4096 App: 0 TCPQ: 0 misc: 0
Approximate # buffers in App 0
Approximate # buffers in App_cp 0
Approximate # buffers in Cache_cp 1023
Approximate # buffers in Cache 30721
Approximate # buffers in Queue 0
Approximate # buffers in misc 0
Approximate # buffers free 100351
Approximate # buffers avail from HW 99309
```

show system resource-usage

Description

Display the minimum and maximum numbers of each type of system resource 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.

Syntax

```
show system resource-usage
```

Mode

All

Usage

To change system resource usage settings, see “system resource-usage” on page 186 command.

Example

The following command shows system resource usage:

```
AX#show system resource-usage
Resource                         Current    Default    Minimum    Maximum
--------------------------------------------------------------------------
l4-session-count                 8388608    8388608    524288     33554432
nat-pool-addr-count              500        500        500        4000
real-server-count                1024       1024       512        2048
real-port-count                  2048       2048       512        4096
service-group-count              512        512        512        1024
virtual-port-count               512        512        256        1024
virtual-server-count             512        512        512        1024
http-template-count              256        256        32         1024
proxy-template-count             128        128        32         128
conn-reuse-template-count        256        256        32         1024
```

```
fast-tcp-template-count          256       256       32        1024
fast-udp-template-count          256       256       32        1024
client-ssl-template-count        256       256       32        1024
server-ssl-template-count        256       256       32        1024
stream-template-count            256       256       32        1024
persist-cookie-template-count    256       256       32        1024
persist-srcip-template-count     256       256       32        1024
class-list-ipv6-addr-count       1024000   2048000   1024000   2048000
```

show tacacs-server

Description Display TACACS statistics.

Syntax **show tacacs-server** [*hostname* | *ipaddr*]

Mode All

Example The following command shows information for TACACS server 5.5.5.5:

```
AX#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 Display or export system information for use when troubleshooting.

Syntax

```
show techsupport
  [export [use-mgmt-port] url]
  [page]
```

Option	Description
export [use-mgmt-port] *url*	Exports the output to a remote server. The *url* specifies the file transfer protocol, username (if required), and directory path.

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL:

tftp://*host/file*

ftp://[*user*@]*host*[:*port*]/*file*

scp://[*user*@]*host/file*

rcp://[*user*@]*host/file*

page Shows the information page by page. Without this option, all the command's output is sent to the terminal at once.

Mode Privileged EXEC level and configuration levels

show terminal

Description Show the terminal settings.

Syntax **show terminal**

Mode All

Example The following command shows the terminal settings.

```
AX#show terminal
Idle-timeout is 00:10:00
Length: 24 lines, Width: 80 columns
Editing is enabled
History is enabled, history size is 256
Auto size is enabled
Terminal monitor is off
```

show tftp

Description Display the currently configured TFTP block size.

Syntax **show tftp**

Mode All

Example The following command shows the TFTP block size.

```
AX(config)#show tftp
TFTP client block size is set to 512
```

show trunk

Description Show information about a trunk group.

Syntax

```
show trunk num
```

Option	Description
num	Trunk number

Mode All

Example The following command shows information for trunk group 1:

```
AX#show trunk 1
Trunk ID          : 1       Member Count: 8
Trunk Status      : Up
Members           : 1   2   3   4   5   6   7   8
Cfg Status        : Enb Enb Enb Enb Enb Enb Enb Enb
Oper Status       : Up  Up  Up  Up  Up  Up  Up  Up
Ports-Threshold   : 6       Timer: 10 sec(s) Running: No
Working Lead      : 1
```

Table 55 describes the fields in the command output.

TABLE 55 show trunk fields

Field	Description
Trunk ID	ID assigned to the trunk by the admin who configured it.
Member Count	Number of ports in the trunk.
Trunk Status	Indicates whether the trunk is up.
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 in order for the trunk to remain up. If the number of up ports falls below the configured threshold, the AX automatically disables the trunk's member ports. The ports are disabled in the running-config. The AX device also generates a log message and an SNMP trap, if these services are enabled.

TABLE 55 show trunk fields (Continued)

Field	Description
Timer	Indicates how many seconds the AX device waits after a port goes down before marking the trunk down, if the ports threshold is exceeded.
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 and for Layer 2 processing. **Note:** If the lead port is shown as 0 or “None”, the trunk interface is down.

show version

Description Display software, hardware, and firmware version information.

Syntax **`show version`**

Mode All

Example The following command shows version information for an AX 2200:

```
AX#show version
AX Series Advanced Traffic Manager AX2500
  Copyright 2007-2011 by A10 Networks, Inc.  All A10 Networks products are
  protected by one or more of the following US patents and patents pending:
  7716378, 7675854, 7647635, 7552126, 20090049537, 20080229418, 20080040789,
  20070283429, 20070271598, 20070180101

      64-bit Advanced Core OS (ACOS) version 2.6.6, build 74 (Oct-05-2011,05:59)
        Booted from Hard Disk secondary image
      Serial Number: AX25011109040041
      aFleX version: 2.0.0
      Hard Disk primary image version 2.6.1-P2, build 114
      Hard Disk secondary image (default) version 2.6.6, build 74
      Compact Flash primary image (default) version 2.4.1, build 139
      Compact Flash secondary image version 2.4.1, build 139
      Last configuration saved at Oct-5-2011, 18:24
      Hardware: 8 CPUs(Stepping 5), Single 74G Hard disk
      Memory 6123 Mbyte, Free Memory 1592 Mbyte
      Current time is Oct-5-2011, 20:03
      The system has been up 0 day, 1 hour, 38 minutes
```

show vlans

Description Display the configured VLANs.

Syntax `show vlans [vlan-id]`

Mode All

Example The following command lists all the VLANs configured on an AX Series device:

```
AX#show vlans
Total VLANs: 2
VLAN 1:
  Untagged Ports:    2   3   4   5   6   7   8   9
                    10  11  12  13  14  15  17  18
                    19  20
    Tagged Ports:   None

VLAN 199:
  Untagged Ports:    1  16
    Tagged Ports:   None
```

show web-service

Description Show settings for Web-management access.

Syntax `show web-service`

Mode All

Example The following command shows the settings for access to the management GUI on an AX Series device:

```
AX#show web-service
AX Web server:
         Idle time:               10 minutes
         Http port:               80
         Https port:              443
         Auto redirect:           Enabled
         Https:                   Enabled
         aXAPI Idle time:         5 minutes
```

Table 56 describes the fields in the command output.

TABLE 56 show web-service fields

Field	Description
Idle time	Number of minutes a web management session can remain idle before the AX device terminates the session.
HTTP port	HTTP port number on which the AX device listens for connections to the management GUI.
HTTPS port	HTTPS port number on which the AX device listens for connections to the management GUI.
Auto redirect	Indicates whether requests for the HTTP port are automatically redirected to the HTTPS port.
HTTPS	State of the HTTPS port on the AX device.
aXAPI Idle time	Number of minutes an aXAPI session can remain idle before bering terminated. Once the aXAPI session is terminated, the session ID generated by the AX device for the session is no longer valid. (Not applicable to IPv6 migration)

AX Debug Commands

The AX debug subsystem enables you to trace packets on the AX device. To access the AX debug subsystem, enter the following command at the Privileged EXEC level of the CLI:

axdebug

The CLI prompt changes as follows:

```
AX(axdebug)#
```

This chapter describes the debug-related commands in the AX debug subsystem.

To perform AX debugging using this subsystem:

1. Use the **filter** command to configure packet filters to match on the types of packets to capture.

2. (Optional) Use the **count** command to change the maximum number of packets to capture.

3. (Optional) Use the **timeout** command to change the maximum number of minutes during which to capture packets.

4. (Optional) Use the **incoming** or **outgoing** command to limit the interfaces on which to capture traffic.

5. Use the **capture** command to start capturing packets. The AX 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.

6. To display capture files, use the **show axdebug file** command. (See “show axdebug file” on page 694.)

7. To export capture files, use the **export axdebug** command at the Privileged EXEC or global configuration level of the CLI. (See “export” on page 67.)

The AXdebug utility creates a debug file in packet capture (PCAP) format. The PCAP format can be read by third-party diagnostic applications such as Wireshark, Ethereal (the older name for Wireshark) and tcpdump. To simplify export of the PCAP file, the AX device compresses it into a zip file in tar format. To use a PCAP file, you must untar it first.

capture

Description Start capturing packets.

Syntax

```
[no] capture parameter
```

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

Default

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

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

Mode

AX debug

Usage

To minimize the impact of packet capture on system performance, A10 Networks recommends 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, see “show axdebug file” on page 694.

Example

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

```
AX(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.

```
AX(axdebug)#capture detail
Wait for debug output, enter <ctrl c> to exit
i( 1, 0, ccae)> ip 10.10.11.30 > 30.30.31.30 tcp 80 > 13638 SA 7ab6ae46:ddb87996(0)
Dump buffer(0xa6657048), len(80 bytes)...
0xa6657048: 00900b0b 3e83001d 09f0dec2 08004500 : ....>.........E.
0xa6657058: 003c0000 40004006 e8580a0a 0b1e1e1e : .<..@.@..X......
0xa6657068: 1f1e0050 35467ab6 ae46ddb8 7996a012 : ...P5Fz..F..y...
0xa6657078: 16a02ea5 00000204 05b40402 080a5194 : ..............Q.
0xa6657088: 6c551f3c 1d3f0103 03072d59 f97f0000 : lU.<.?....-Y....
0xa6657098: 00000000 00000000 00000000 00000000 : ................
o( 3, 0, ccae)> ip 10.10.11.30 > 30.30.31.30 tcp 80 > 13638 SA 7ab6ae46:ddb87996(0)
Dump buffer(0xa6657048), len(80 bytes)...
0xa6657048: 001d09f0 e01e0090 0b0b3e83 08004500 : ..........>...E.
0xa6657058: 003c0000 40003f06 e9580a0a 0b1e1e1e : .<..@.?..X......
0xa6657068: 1f1e0050 35467ab6 ae46ddb8 7996a012 : ...P5Fz..F..y...
0xa6657078: 16a02ea5 00000204 05b40402 080a5194 : ..............Q.
0xa6657088: 6c551f3c 1d3f0103 03072d59 f97f0000 : lU.<.?....-Y....
0xa6657098: 00000000 00000000 00000000 00000000 : ................
i( 1, 0, ccaf)> ip 10.10.11.30 > 30.30.31.30 tcp 80 > 13638 A 7ab6ae47:ddb87a2b(0)
Dump buffer(0xa6657848), len(80 bytes)...
0xa6657848: 00900b0b 3e83001d 09f0dec2 08004500 : ....>.........E.
0xa6657858: 0034c211 40004006 264f0a0a 0b1e1e1e : .4..@.@.&O......
0xa6657868: 1f1e0050 35467ab6 ae47ddb8 7a2b8010 : ...P5Fz..G..z+..
0xa6657878: 00367344 00000101 080a5194 6c561f3c : .6sD......Q.lV.<
0xa6657888: 1d4041de e3380000 00000000 00000000 : .@A..8..........
0xa6657898: 00000000 00000000 00000000 00000000 : ................
...
```

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

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

count

Description Specify the maximum number of packets to capture.

Syntax

```
[no] count num
```

Parameter	Description
num.	Maximum number of packets to capture, 0-65535. To capture an unlimited number of packets, specify 0.

Default 3000

Mode AX debug

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

```
AX(axdebug)#count 2048
```

delete

Description Delete an axdebug capture file.

Syntax

```
delete filename
```

Default N/A

Mode AX debug

Example The following command deletes capture file “file123”:

```
AX(axdebug)#delete file123
```

filter

Description Configure an AX debug filter, to specify the types of packets to capture.

Syntax

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

Parameter	Description
filter-id	ID of the filter, 1-255.

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

Command	Description
dst {**ip** *ipaddr* | **mac** *macaddr* | **port** *portnum*}	Matches on the specified destination IP address, MAC address, or protocol port number.
l3-proto {**arp** | **ip** | **ipv6**}	Matches on the specified Layer 3 protocol.
ip *ipaddr* {*subnet-mask* | */mask-length*}	Matches on the specified IPv4 address.
mac *macaddr*	Matches on the specified MAC address.
offset *position* **length** *bytes* *operator value*	Matches on the specified length of bytes and value of those bytes within the packet. *position* – Starting position within the packet, 1-65535 bytes. *bytes* – Number of consecutive bytes to filter on, from 1-65535, beginning at the offset position. *operator* – One of the following: **>** (greater than) **>=** (greater than or equal to) **<=** (smaller than or equal to) **<** (smaller than) **=** (equal to)

range *min-value* *max-value* (select a range)

value – String to filter on.

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

Default

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

Mode

AX debug

Usage

If a packet capture is running and you change the filter, there will be a 5-second delay while the AX 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 AX debug 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.

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

outgoing [portnum ...]
```

Default

Disabled

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

Mode

AX debug

Example

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

```
AX(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 AX debug filters.

```
AX(axdebug)#outgoing 7
```

length

Description

Specify the maximum length of packets to capture. Packets that are longer are not captured.

Syntax

```
[no] length bytes
```

Parameter	Description
bytes	Maximum packet length, 64-1518 bytes.

Default

1518

Mode

AX debug

Example The following command changes the maximum packet length to capture to 128:

```
AX(axdebug)#length 128
```

maxfile

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

Syntax

```
[no] maxfile num
```

Parameter	Description
num	Maximum number of files to keep, 1-65535.

Default 100

Mode AX debug

Usage Once the maximum is reached, new axdebug files can not be created until existing files are removed.

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

```
AX(axdebug)#maxfile 125
```

outgoing

Description See “incoming | outgoing” on page 796.

timeout

Description Specify the maximum number of minutes to capture packets.

Syntax

```
[no] timeout minutes
```

Parameter	Description
minutes	Maximum number of minutes to capture packets, 0-65535.

Default 5

Mode AX debug

Example

The following command changes the capture timeout to 10 minutes:

```
AX(axdebug)#timeout 10
```

show health stat Up / Down Causes

This chapter lists the cause strings for the numeric cause codes that appear in the Up and Down fields of **show health stat** output. The Up / Down cause codes are shown in the output under “Cause(Up/Down/Retry)”.

Up Causes

Table 57 lists the Up causes.

TABLE 57 show health stat Up Causes

Cause Code	Cause String
0	HM_INVALID_UP_REASON
1	HM_DNS_PARSE_RESPONSE_OK
2	HM_EXT_REPORT_UP
3	HM_EXT_TCL_REPORT_UP
4	HM_FTP_ACK_USER_LOGIN
5	HM_FTP_ACK_PASS_LOGIN
6	HM_HTTP_RECV_URL_FIRST
7	HM_HTTP_RECV_URL_NEARBY_FIRST
8	HM_HTTP_RECV_URL_FOLLOWING
9	HM_HTTP_RECV_URL_NEARBY_FOLLOWING
10	HM_HTTP_STATUS_CODE
11	HM_ICMP_RECV_OK
12	HM_ICMP_RECV6_OK
13	HM_LDAP_RECV_ACK
14	HM_POP3_RECV_ACK_PASS_OK
15	HM_RADIUS_RECV_OK
16	HM_RTSP_RECV_STATUS_OK
17	HM_SIP_RECV_OK
18	HM_SMTP_RECV_OK
19	HM_SNMP_RECV_OK
20	HM_TCP_VERIFY_CONN_OK
21	HM_TCP_CONN_OK
22	HM_TCP_HALF_CONN_OK
23	HM_UDP_RECV_OK
24	HM_UDP_NO_RESPOND
25	HM_COMPOUND_UP

Down Causes

Table 58 lists the Down causes.

TABLE 58 show health stat Down Causes

Cause Code	Cause String
0	HM_INVALID_DOWN_REASON
1	HM_DNS_TIMEOUT
2	HM_EXT_TIMEOUT
3	HM_EXT_TCL_TIMEOUT
4	HM_FTP_TIMEOUT
5	HM_HTTP_TIMEOUT
6	HM_HTTPS_TIMEOUT
7	HM_ICMP_TIMEOUT
8	HM_LDAP_TIMEOUT
9	HM_POP3_TIMEOUT
10	HM_RADIUS_TIMEOUT
11	HM_RTSP_TIMEOUT
12	HM_SIP_TIMEOUT
13	HM_SMTP_TIMEOUT
14	HM_SNMP_TIMEOUT
15	HM_TCP_TIMEOUT
16	HM_TCP_HALF_TIMEOUT
17	HM_DNS_RECV_ERROR
18	HM_DNS_PARSE_RESPONSE_ERROR
19	HM_DNS_RECV_LEN_ZERO
20	HM_EXT_WAITPID_FAIL
21	HM_EXT_TERM_BY_SIG
22	HM_EXT_REPORT_DOWN
23	HM_EXT_TCL_REPORT_DOWN
24	HM_FTP_RECV_TIMEOUT
25	HM_FTP_SEND_TIMEOUT
26	HM_FTP_NO_SERVICE
27	HM_FTP_ACK_USER_WRONG_CODE
28	HM_FTP_ACK_PASS_WRONG_CODE
29	HM_COM_CONN_CLOSED_IN_WRITE
30	HM_COM_OTHER_ERR_IN_WRITE
31	HM_COM_CONN_CLOSED_IN_READ
32	HM_COM_OTHER_ERR_IN_READ
33	HM_COM_SEND_TIMEOUT
34	HM_COM_CONN_TIMEOUT
35	HM_COM_SSL_CONN_ERR

TABLE 58 show health stat Down Causes (Continued)

Cause Code	Cause String
36	HM_HTTP_SEND_URL_ERR
37	HM_HTTP_RECV_URL_ERR
38	HM_HTTP_RECV_MSG_ERR
39	HM_HTTP_NO_LOCATION
40	HM_HTTP_WRONG_STATUS_CODE
41	HM_HTTP_WRONG_CHUNK
42	HM_HTTP_AUTH_ERR
43	HM_HTTPS_SSL_WRITE_ERR
44	HM_HTTPS_SSL_WRITE_OTHERS
45	HM_HTTPS_SSL_READ_ERR
46	HM_HTTPS_SSL_READ_OTHERS
47	HM_ICMP_RECV_ERR
48	HM_ICMP_SEND_ERR
49	HM_ICMP_RECV6_ERR
50	HM_LDAP_RECV_ACK_ERR
51	HM_LDAP_SSL_READ_ERR
52	HM_LDAP_SSL_READ_OTHERS
53	HM_LDAP_RECV_ACK_WRONG_PACKET
54	HM_LDAP_SSL_WRITE_ERR
55	HM_LDAP_SSL_WRITE_OTHERS
56	HM_LDAP_SEND_ERR
57	HM_POP3_RECV_TIMEOUT
58	HM_POP3_SEND_TIMEOUT
59	HM_POP3_NO_SERVICE
60	HM_POP3_RECV_ACK_USER_ERR
61	HM_POP3_RECV_ACK_PASS_ERR
62	HM_RADIUS_RECV_ERR
63	HM_RADIUS_RECV_ERR_PACKET
64	HM_RADIUS_RECV_NONE
65	HM_RTSP_RECV_STATUS_ERR
66	HM_RTSP_RECV_ERR
67	HM_RTSP_SEND_ERR
68	HM_SIP_RECV_ERR
69	HM_SIP_RECV_ERR_PACKET
70	HM_SIP_CONN_CLOSED
71	HM_SIP_NO_MEM
72	HM_SIP_STARTUP_ERR
73	HM_SMTP_RECV_ERR
74	HM_SMTP_NO_SERVICE
75	HM_SMTP_SEND_HELO_TIMEOUT
76	HM_SMTP_SEND_QUIT_TIMEOUT

TABLE 58 show health stat Down Causes (Continued)

Cause Code	Cause String
77	HM_SMTP_WRONG_CODE
78	HM_SNMP_RECV_ERR
79	HM_SNMP_RECV_ERR_PACKET
80	HM_SNMP_RECV_ERR_OTHER
81	HM_TCP_PORT_CLOSED
82	HM_TCP_ERROR
83	HM_TCP_INVALID_TCP_FLAG
84	HM_TCP_HALF_NO_ROUTE
85	HM_TCP_HALF_NO_MEM
86	HM_TCP_HALF_SEND_ERR
87	HM_UDP_RECV_ERR
88	HM_UDP_RECV_ERR_OTHERS
89	HM_UDP_NO_SERVICE
90	HM_UDP_ERR
91	HM_COMPOUND_INVAL_RPN
92	HM_COMPOUND_DOWN
93	HM_COMPOUND_TIMEOUT

Customer Driven Innovation

Corporate Headquarters

A10 Networks, Inc.
3 West Plumeria Dr.
San Jose, CA 95134 USA

Tel: +1-408-325-8668 (main)
Tel: +1-408-325-8676 (support - worldwide)
Tel: +1-888-822-7210 (support - toll-free in USA)
Fax: +1-408-325-8666

www.a10networks.com