Commands Reference — ACLI
Avaya Ethernet Routing Switch 8300

4.2
NN46200-104, 02.05
November 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release 25
- Features 25
  - STP BPDU filtering 25
  - IP spoof detection 25
  - IPFIX 26
  - DHCP snooping 26
  - Dynamic ARP inspection 27
  - IP Source Guard 27
  - BGP Lite 27
  - IGMPv3 snoop 28
- Other changes 28
  - Customer service 29

Chapter 2: Introduction 31
- Navigation 31

Chapter 3: Utility management commands 33
- Navigation 33
- attribute 34
- boot 35
- cd 36
- chkdisk 36
- clear 37
- copy 38
- cp 39
- date 39
- delete 40
- dir 40
- disable 41
- edit 41
- enable 42
- end 42
- exit 42
- format 43
- format-flash 43
- grep 43
- help 44
- history 44
- install 45
- logout 45
- mkdir 45
- more 46
- mv 46
- pcmcia-stop 47
- peer 47
- ping 48

pwd ... 49
reload ... 49
rename ... 50
rlogin ... 50
rlogin-sessions ... 51
rsh ... 51
save ... 52
show running-config ... 52
source ... 53
sys-action ... 53
telnet ... 54
telnet-access ... 54
test in loopback ... 55
test ... 55
trace ... 56
trace auto ... 57
traceroute ... 58
write memory ... 59
Chapter 4: Boot config commands ... 61
Navigation ... 61
boot choice license-file ... 64
boot config bootp ... 64
boot config choice config-file ... 65
boot config choice image-file ... 65
boot config cli more ... 66
no boot config cli more ... 66
boot config cli prompt ... 67
boot config cli rlogin-sessions ... 67
boot config cli screenlines ... 68
boot config cli telnet-sessions ... 68
boot config cli timeout ... 69
boot config delay ... 69
boot config flags ... 70
no boot config flags ... 72
boot config flags autoboot ... 73
no boot config flags autoboot ... 74
boot config flags block-snmp ... 74
no boot config flags block-snmp ... 74
boot config flags daylight-saving-time ... 74
no boot config flags daylight-saving-time ... 75
boot config flags debug-config ... 75
no boot config flags debug-config ... 75
boot config flags debugmode ... 76
no boot config flags debugmode ... 76
boot config flags factorydefaults ... 76
no boot config flags factorydefaults ... 77
boot config flags ftpd ... 77

no boot config flags ftpd 77
boot config flags info 78
boot config flags logging 78
no boot config flags logging 78
boot config flags nncli 78
no boot config flags nncli 79
boot config flags reboot 79
no boot config flags reboot 79
boot config flags rlogind 80
no boot config flags rlogind 80
boot config flags savetostandby 80
no boot config flags savetostandby 81
boot config flags telnetd 81
no boot config flags telnetd 81
boot config flags tftpd 81
no boot config flags tftpd 82
boot config flags trace-logging 82
no boot config flags trace-logging 82
boot config flags verify-config 83
no boot config flags verify-config 83
boot config flags wdt 83
no boot config flags wdt 84
boot config host ftp-debug 84
no boot config host ftp-debug 84
boot config host password 85
boot config host tftp-debug 85
no boot config host tftp-debug 86
boot config host tftp-hash 86
no boot config host tftp-hash 86
boot config host tftp-rexmit 87
boot config host tftp-timeout 87
boot config host user 88
boot config master 88
boot config net autonegotiate 89
no boot config net autonegotiate 89
boot config net bootp 90
no boot config net bootp 90
boot config net fullduplex 91
no boot config net fullduplex 91
boot config net ip 92
boot config net restart 93
boot net route 93
boot config net speed 94
boot config net tftp 95
boot config sio 95
boot config sio 8databits 96
no boot config sio 8databits 96

boot config sio baud ... 97
boot config sio disable ... 97
boo tconfig sio enable ... 97
boot config sio info ... 98
boot config sio mode ... 98
boot config sio mtu ... 98
boot config sio my-ip ... 99
boot config sio peer-ip ... 99
boot config sio pppfile ... 100
boot config sio restart ... 100
boot config sio slip-compression ... 101
no boot config sio slip-compression ... 101
boot config sio slip-rx-compression ... 101
no boot config sio slip-rx-compression ... 102
Chapter 5: System management commands ... 103
Navigation ... 103
auto-recover-delay ... 104
default auto-recover-delay ... 104
no auto-recover-delay ... 105
autotopology ... 105
no autotopology ... 105
banner ... 106
no banner ... 106
clock set ... 107
clock-sync-time ... 107
enable ... 108
link-flap-detect ... 108
no link-flap-detect auto-port-down ... 109
no link-flap-detect send-trap ... 109
load-module ... 110
logging ... 110
loginprompt ... 111
no loginprompt ... 112
mgmt-virtual-ip ... 112
no mgmt-virtual-ip ... 113
monitor-stats ... 113
more ... 114
no more ... 114
msg-control ... 114
no msg-control ... 115
mtu ... 115
passwordprompt ... 115
no passwordprompt ... 116
portlock ... 116
prompt ... 116
rlogin-sessions ... 117
screenlines ... 117

shutdown ... 118
no shutdown ... 118
sys-action cpuswitchover ... 118
sys-action resetconsole ... 119
sys-action resetcounters ... 119
udpsrc-by-vip ... 119
no udpsrc-by-vip ... 120
Chapter 6: SNMP commands ... 121
Navigation ... 121
snmp-server authentication-trap ... 122
no snmp-server authentication-trap ... 122
snmp-server bootstrap ... 122
snmp-server community ... 123
snmp-server community name ... 123
snmp-server community security ... 124
no snmp-server community ... 124
snmp-server contact ... 125
snmp-server group ... 125
no snmp-server group ... 126
snmp-server host ... 126
no snmp-server host ... 127
snmp-server location ... 127
snmp-server member ... 128
no snmp-server member ... 128
snmp-server name ... 129
snmp-server user ... 130
no snmp-server user ... 130
snmp-server view ... 131
no snmp-server view ... 132
Chapter 7: Ethernet port commands ... 133
Navigation ... 133
action ... 134
auto-negotiate ... 135
no auto-negotiate ... 135
auto-recover-port ... 136
default auto-recover-port ... 136
no auto-recover-port ... 137
bcast-mcast-rate-limit ... 137
cp-limit ... 138
no cp-limit ... 138
default-vlan-id ... 139
duplex ... 140
eapol ... 140
no eapol ... 142
encapsulation ... 143
no encapsulation ... 143
linktrap ... 144

no linktrap ... 144
lock ... 145
no lock ... 145
name ... 146
shutdown ... 146
no shutdown ... 147
boot config flags spanning-tree-mode ... 147
no boot config flags spanning-tree-mode ... 148
spanning-tree bpdu-filtering ... 148
no spanning-tree bpdu-filtering ... 148
spanning-tree bpdu-filtering timeout ... 149
no spanning-tree bpdu-filtering timeout ... 149
default spanning-tree bpdu-filtering ... 150
show spanning-tree bpdu-filtering ... 151
spanning-tree mstp ... 151
show spanning-tree mstp config ... 152
spanning-tree mstp cist ... 153
no spanning-tree mstp cist ... 153
spanning-tree mstp msti ... 154
show spanning-tree mstp msti config ... 154
spanning-tree mstp msti ... 155
show spanning-tree mstp port ... 155
show spanning-tree mstp status ... 156
spanning-tree rstp ... 156
no spanning-tree rstp ... 157
show spanning-tree rstp config ... 157
show spanning-tree rstp status ... 158
spanning-tree rstp on port ... 158
no spanning-tree rstp on port ... 159
show spanning-tree rstp port ... 159
tx-queue ... 160
no tx-queue ... 160
unknown-mac-discard ... 161
no unknown-mac-discard ... 162
test loopback ... 163
test stop ... 163
untagged-frames-discard ... 164
no untagged-frames-discard ... 164
Chapter 8: Security commands ... 165
Navigation ... 165
access-policy disable ... 167
access-policy enable ... 167
access-policy info ... 167
access-policy policy ... 167
access-policy policy create ... 169
access-policy policy info ... 170
default ip dhcp-snooping ... 171

eapol default-guest-vlan ... 171
eapol guest-vlan ... 171
eapol allow-non-eap mac-max ... 172
eapol non-eap-mac add ... 172
no eapol guest-vlan ... 172
eapol guest-vlan-id ... 172
eapol multihost ... 173
eapol guest-vlan ... 173
eapol multihost mac-max ... 173
eapol allow-non-eap ... 173
ip arp-inspection vlan ... 174
ip arp-inspection ... 174
ip dhcp-snooping (global) ... 175
ip dhcp-snooping (interface) ... 175
ip dhcp-snooping vlan ... 176
ip verify source interface ... 176
no access-policy policy ... 177
no eapol allow-non-eap ... 177
no eapol guest-vlan ... 177
no eapol multihost ... 178
no eapol non-eap-mac ... 178
no ip arp-inspection vlan ... 178
no ip dhcp-snooping ... 179
no ip dhcp-snooping vlan ... 179
no ip verify source interface ... 179
no nsna ... 180
no nsna enable ... 180
no nsna nsnas ... 180
no nsna phone-signature ... 181
no nsna vlan ... 181
no radius ... 182
no radius-server ... 182
no snmp-server v1v2 community ... 182
no syslog host ... 183
nsna ... 183
nsna enable ... 184
nsna nsnas ... 184
nsna phone-signature ... 185
nsna uplink vlans ... 185
nsna vlan color ... 186
nsna fail-open vlan-id ... 186
nsna fail-open enable ... 187
no nsna fail-open ... 187
radius ... 187
radius clear-stat ... 188
radius info ... 189
radius-server info ... 189

snmp-server group info ... 189
snmp-server group match ... 189
snmp-server group view ... 190
snmp-server info ... 191
snmp-server member info ... 191
snmp-server member name ... 192
snmp-server user auth ... 192
snmp-server user info ... 193
snmp-server user priv ... 193
snmp-server view info ... 194
snmp-server view mask ... 194
snmp-server view type ... 195
syslog host ... 196
syslog host create ... 196
syslog host severity ... 197
Chapter 9: IP protocol commands ... 199
Navigation ... 199
accept adv-rtr ... 202
area ... 203
as-boundary-router enable ... 204
default as-boundary-router enable ... 204
no as-boundary-router enable ... 204
auto-vlink enable ... 205
default-metric ... 205
default default-metric ... 206
default timer basic ... 206
host-route ... 207
interface loopback ... 207
ip address ... 208
no ip address ... 208
ip alternative-route ... 209
no ip alternative-route ... 209
ip arp ... 209
no ip arp ... 210
ip arp proxy ... 211
no ip arp proxy ... 211
ip arp response ... 211
no ip arp response ... 211
ip default-ttl ... 212
ip dhcp-relay broadcast ... 212
ip dhcp-relay ... 213
ip dhcp-relay max-hop ... 213
ip dhcp-relay min-sec ... 214
ip dhcp-relay mode ... 214
ip dhcp-relay fwd-path ... 214
ip ipfix (global) ... 215
no ip ipfix enable ... 216

no ip ipfix collector ... 216
no ip ipfix exporter-enable ... 217
ip ipfix (port) ... 217
no ip ipfix (port) ... 218
clear ip ipfix stats ... 218
ip forward-protocol udp ... 218
no ip forward-protocol udp ... 219
ip forward-protocol udp portfwdlist ... 219
no ip forward-protocol udp portfwdlist ... 220
ip forward-protocol udp ... 221
no ip forward-protocol udp ... 222
ip icmp-unreach-msg ... 223
no ip icmp-unreach-msg ... 223
ip irdp enable ... 223
no ip irdp enable ... 223
ip irdp ... 224
no ip irdp ... 224
default ip irdp ... 225
no ip irdp multicast ... 225
ip irdp vlan multicast ... 225
no ip irdp vlan multicast ... 226
ip more-specific-non-local-route enable ... 226
no ip more-specific-non-local-route enable ... 226
ip ospf ... 227
ip ospf spf-run ... 228
ip prefix-list ... 229
no ip prefix-list ... 230
ip routing ... 230
no ip routing ... 230
ip rip ... 230
ip route ... 234
no ip route ... 235
ip route preference protocol ... 235
net6-mgmt ipv6 ... 236
no net6-mgmt ipv6 ... 237
no net6-mgmt ipv6 route ... 237
net6-mgmt ipv6 route ... 238
ipv6 mgmt-virtual ... 238
lldp ... 239
default lldp ... 239
lldp port status ... 240
no lldp port ... 240
default lldp port ... 240
lldp port status ... 241
no lldp status ... 241
default lldp port ... 241
lldp tx-tlv ... 242

no lldp tx-tlv ... 242
default lldp tx-tlv ... 243
lldp tx-tlv dot1 ... 243
no lldp tx-tlv dot1 ... 244
default lldp tx-tlv dot1 ... 244
lldp tx-tlv dot3 ... 244
no lldp tx-tlv dot3 ... 245
default lldp tx-tlv dot3 ... 245
lldp tx-tlv med ... 246
no lldp tx-tlv med ... 246
default lldp tx-tlv med ... 247
lldp location-identification civic-address ... 247
manualtrigger ip rip interface vlan ... 248
network ... 249
no network ... 249
network area ... 250
redistribute enable ... 250
redistribute source ... 251
route-map ... 251
no route-map ... 253
router ospf ... 254
router ospf enable ... 254
no router ospf enable ... 254
router rip ... 255
router rip enable ... 255
no router rip enable ... 255
router-id ... 256
slpp ... 256
Default slpp ... 257
no slpp ... 257
slpp port ... 258
default slpp port ... 258
no slpp port ... 259
spoof-detect ... 259
no spoof-detect ... 260
show spoof-detect ... 260
timer basic ... 261
timers basic holddown ... 262
trap enable ... 263
vlan nlb-mode ... 263
no vlan nlb-mode ... 264
Chapter 10: Layer 2 and 3 operations commands ... 265
Navigation ... 265
bcast-mcast-rate-limit enable ... 267
ist ... 268
no ist ... 268
ist enable ... 269

no ist enable ... 269
no mlt encapsulation dot1q ... 269
no mlt name ... 270
interface mlt ... 270
smlt ... 270
no smlt ... 271
ip rsmlt ... 271
default ip rsmlt ... 272
no ip rsmlt ... 272
mlt members ... 272
mlt add-vlan ... 273
mlt name ... 273
no mlt members ... 274
mlt remove-vlan ... 274
mlt create ... 275
mlt encapsulation ... 275
no mlt encapsulation ... 276
no mlt ... 276
spanning-tree stp ... 277
spanning-tree stp add-ports ... 278
spanning-tree stp create ... 278
spanning-tree stp remove-ports ... 279
no spanning-tree ... 279
telnet-access ... 280
vlan action ... 280
vlan add-mlt ... 281
vlan members ... 281
vlan name ... 282
vlan qos-level ... 283
no vlan ... 283
vlan create type port ... 284
vlan create type protocol-ApltkEther2Snap ... 284
vlan create type protocol-decEther2 ... 285
vlan create type protocol-decOtherEther2 ... 286
vlan create type protocol-ipEther2 ... 286
vlan create type protocol-ipv6Ether2 ... 287
vlan create type protocol-ipx802.2 ... 288
vlan create type protocol-ipx802.3 ... 289
vlan create type protocol-ipxEther2 ... 289
vlan create type protocol-ipxSnap ... 290
vlan create type protocol-Netbios ... 291
vlan create type protocol-RarpEther2 ... 291
vlan create type protocol-sna802.2 ... 292
vlan create type protocol-snaEther2 ... 293
vlan create type protocol-Userdef ... 294
vlan create type protocol-vinesEther2 ... 294
vlan create type protocol-xnsEther2 ... 295

vlan fdb-entry aging-time ... 296
vlan fdb-entry flush ... 296
vlan fdb-entry qos-level ... 297
vlan fdb-entry sync ... 297
vlan fdb-filter add ... 298
no vlan fdb-filter ... 299
vlan fdb-static add ... 299
no vlan fdb-static ... 300
vlan static-mcastmac add ... 300
vlan static-mcastmac add-mlt ... 301
vlan static-mcastmac remove-mlt ... 301
vlan static-mcastmac add-ports ... 302
vlan static-mcastmac remove ... 302
vlan static-mcastmac remove-mlt ... 303
vlan static-mcastmac remove-ports ... 304
no vlan static-mcastmac ... 304
interface vlan ... 305
ip address ... 305
ip vrf ... 306
vrf ... 306
Chapter 11: Route filters commands ... 307
Navigation ... 307
filter acl ip ... 308
filter acl non-ip ... 308
filter acl action ... 309
filter acl ace ... 311
no filter acl ace ... 312
no filter acl ... 313
show filter acl advanced ... 313
filter acl ethernet ... 314
filter acl ip-hdr ... 315
filter acl port ... 317
filter acl protocol ... 318
filter acl debug ... 319
filter acg ... 320
filter acg modify ... 320
no filter acg ... 321
filter act ethernet ... 321
filter act ip-hdr ... 323
no filter act ... 326
filter act ... 326
filter act pattern ... 327
no filter act pattern ... 328
show filter act ... 328
Chapter 12: Test and diagnostic commands ... 329
Navigation ... 329
clear port-stats ... 330

clear telnet ... 330
port-mirroring ... 331
no port-mirroring ... 332
rmon alarm ... 332
no rmon alarm ... 333
rmon event ... 334
no rmon event ... 334
rmon history ... 335
no rmon history ... 336
rmon memsize ... 336
rmon stats ... 337
no rmon stats ... 337
rmon trap-option ... 338
rmon util-method ... 338
test ... 339
trace auto-enable ... 339
trace auto-enable add-module ... 340
trace auto-enable auto-trace ... 341
trace auto-enable remove-module ... 342
trace clear ... 342
trace filter ... 343
trace grep ... 343
trace level ... 343
trace off ... 344
trace route-policy ... 344
trace screen ... 345
traceroute ... 345
vct test ... 346
Chapter 13: Multicast services commands ... 347
Navigation ... 347
debug ip pim ... 349
interface vlan ... 350
ip igmp ... 350
ip igmp access-filter ... 351
no ip igmp access-filter ... 352
ip igmp compatibility-mode ... 353
no ip igmp compatibility-mode ... 353
default ip igmp compatibility-mode ... 353
ip igmp dynamic-downgrade-version ... 353
no ip igmp dynamic-downgrade-version ... 354
default ip igmp dynamic-downgrade-version ... 354
ip igmp fast-leave ... 354
no ip igmp fast-leave ... 355
ip igmp fast-leave-members ... 355
no ip igmp fast-leave-members ... 355
ip igmp flush ... 356
ip igmp immediate-leave-mode ... 357

default ip igmp immediate-leave-mode 357
ip igmp mrouter 357
no ip igmp mrouter 358
ip igmp multicast-vlan-registration 358
no ip igmp multicast-vlan-registration 359
ip igmp multicast-vlan-registration receiver-vlan 359
no ip igmp multicast-vlan-registration receiver-vlan 359
ip igmp proxy-snoop 360
no ip igmp proxy-snoop 360
ip igmp router-alert 361
no ip igmp router-alert 361
ip igmp snoop 361
no ip igmp snoop 362
ip igmp static-members 362
no ip igmp static-members 363
ip igmp 363
no ip igmp 365
default ip igmp 368
ip igmp generate-log 370
no ip igmp generate-log 370
default ip igmp generate-log 370
ip igmp generate-trap 371
no ip igmp generate-trap 371
default ip igmp generate-trap 371
ip igmp mrdisc 372
no ip igmp mrdisc 372
default ip igmp mrdisc 373
ip igmp snoop-querier 373
no ip igmp snoop-querier 373
ip igmp snoop-querier-addr 373
no ip igmp snoop-querier-addr 374
ip igmp ssm dynamic-learning 374
no ip igmp ssm dynamic-learning 374
default ip igmp ssm dynamic-learning 375
ip igmp ssm group-range 375
ip igmp ssm-map 375
ip igmp ssm-map enable 376
no ip igmp ssm-map enable 376
no ip igmp ssm-map 376
ip igmp ssm-map all 377
no ip igmp ssm-map all 377
ip igmp stream-limit 377
no ip igmp stream-limit 378
ip igmp stream-limit-group enable max-streams 378
no ip igmp stream-limit-group 379
default ip igmp stream-limit-group 379
ip igmp stream-limit-max-streams 380

default ip igmp stream-limit-max-streams 380
ip mroute static-source-group 380
no ip mroute static-source-group 381
ip pim 382
Configuring PIM-SM globally 382
Configuring PIM-SM on a VLAN 384
ip pim enable 385
Enabling PIM-SM globally 385
Enabling PIM-SM on a VLAN 385
no ip pim 385
Disabling PIM-SM globally 386
Disabling PIM-SM on a VLAN 386
ip pim interface virtual neighbor 386
no ip pim interface virtual neighbor 387
ip pim rp-candidate group rp 387
no ip pim rp-candidate group rp 388
ip pim static-rp 388
no ip pim static-rp 389
ip pim static-rp 389
no ip pim static-rp 390
Chapter 14: Quality of Service commands 391
Navigation 391
interface FastEthernet/GigabitEthernet 392
qos 392
qos 8021p-override 393
no qos 8021p-override 393
qos shaper 394
qos shaper rate 394
qos shaper burst size 394
no qos shaper 395
qos trust-dscp enable 395
no qos trust-dscp enable 395
qos update-dynamic-mac-qos-level 396
no qos update-dynamic-mac-qos-level 396
qos map 396
qos policy create 398
no qos policy 399
qos policy action 399
no qos policy action 400
qos policy modify 401
qos egress-counter-set 402
no qos egress-counter-set 403
qos map-qos-level-override 403
Chapter 15: Web server commands 405
Navigation 405
web-server 405
web-server password 406

no web-server ... 406
Chapter 16: PoE commands ... 407
Navigation ... 407
interface FastEthernet/GigabitEthernet ... 407
interface FastEthernet ... 408
poe detect-control ... 408
poe detection-control ... 409
poe fw-upgrade slot ... 409
poe limit ... 410
poe limit in interface mode ... 410
poe notification slot ... 410
no poe notification ... 411
poe port admin ... 411
poe priority ... 411
poe priority in interface mode ... 412
poe priority in global config mode ... 412
poe shutdown ... 413
no poe shutdown ... 413
poe shutdown in global config mode ... 413
no poe shutdown in interface GigabitEthernet mode ... 414
no poe shutdown ... 414
poe type ... 414
poe type port ... 415
poe usage-threshold ... 415
Chapter 17: LACP commands ... 417
Navigation ... 417
lacp ... 417
no lacp ... 419
show lacp interface ... 419
lacp on port ... 420
no lacp on port ... 422
show vlacp ... 422
vlacp enable ... 423
default vlacp enable ... 423
no vlacp enable ... 423
vlacp macaddress ... 423
default vlacp macaddress ... 424
no vlacp macaddress ... 425
vlacp on a port ... 425
default vlacp on a port ... 426
no vlacp enable on a port ... 426
show vlacp interface ... 427
lacp enable on an mlt ... 427
no lacp on an mlt ... 428
show mlt ... 428
Chapter 18: BGP Lite commands ... 429
Navigation ... 429

aggregate-address ... 432
default aggregate-address ... 433
no aggregate-address ... 434
auto-peer-restart enable ... 435
default auto-peer-restart enable ... 435
no auto-peer-restart enable ... 435
auto-summary ... 436
default auto-summary ... 436
no auto-summary ... 436
bgp aggregation enable ... 436
default bgp aggregation enable ... 437
no bgp aggregation enable ... 437
bgp client-to-client reflection ... 437
default bgp client-to-client reflection ... 438
no bgp client-to-client reflection ... 438
bgp cluster-id ... 438
no bgp cluster-id ... 439
bgp default local-preference ... 439
default bgp default local-preference ... 440
no bgp default local-preference ... 440
bgp multiple-paths ... 440
default bgp multiple-paths ... 441
debug-screen ... 441
default debug-screen ... 441
no debug-screen ... 442
default-information originate ... 442
default default-information originate ... 442
no default-information originate ... 442
global-debug mask ... 443
default global-debug mask ... 444
no global-debug mask ... 444
ibgp-report-import-rt enable ... 444
default ibgp-report-import-rt enable ... 445
no ibgp-report-import-rt enable ... 445
ignore-illegal-rtrid enable ... 445
default ignore-illegal-rtrid enable ... 446
no ignore-illegal-rtrid enable ... 446
neighbor ... 446
default neighbor ... 449
no neighbor ... 451
neighbor-debug-all mask ... 453
network ... 454
default network ... 455
no network ... 455
no-med-path-is-worst enable ... 456
default no-med-path-is-worst enable ... 456
no no-med-path-is-worst enable ... 456

quick-start enable 456
default quick-start enable 457
no quick-start enable 457
redistribute 457
default redistribute 458
no redistribute 458
route-reflector enable 459
default route-reflector enable 459
no route-reflector enable 460
route-refresh 460
default route-refresh 460
no route-refresh 460
router-id 461
no router-id 461
synchronization 461
default synchronization 462
no synchronization 462
traps enable 462
default traps enable 462
no traps enable 463
router bgp 463
no router bgp enable 463
neighbor 464
no neighbor 467
default neighbor 469
neighbor password 470
no neighbor password 471
default neighbor password 471
redistribute 472
default redistribute 473
ip bgp apply redistribute 473
no redistribute 473
ip as-list 474
no ip as-list 475
ip community-list 475
no ip community-list 476
ip bgp restart-bgp 477
ip bgp stats-clear-counters 477
ip bgp stats-clear-counters neighbor 478
show ip bgp aggregates 478
show ip bgp cidr-only 478
show ip bgp conf 479
show ip bgp neighbors 479
show ip bgp networks 480
show ip bgp peer-group 480
show ip bgp route 481
show ip bgp redistributed-routes 481

show ip bgp summary ... 482
show ip bgp stats ... 482
Chapter 19: Show commands ... 483
Navigation ... 483
show vct ... 487
show poe main-status|port-stats|port-status|power-measurement|sys-status ... 488
show web-server ... 488
show qos egress-counter-set|egress-stats|mac-qos-level-override|map|policy|policy-remark-dp|policy-stats ... 489
show ip pim active-rp|bsr|interface|mode|mroute|neighbor|rp-candidate|rp-hash|static-rp|virtual-neighbor ... 490
show debug ip pim ... 491
show interfaces vlan ip ... 491
show ip igmp ... 492
show ip igmp ssm ... 493
show ip igmp ssm-map ... 493
show ip arp-inspection vlan ... 493
show ip arp-inspection interface ... 493
show ip igmp interface vlan ... 494
show ip igmp multicast-vlan-registration group ... 494
show ip igmp multicast-vlan-registration vlan ... 495
show ip dhcp-relay fwd-path ... 495
show ip dhcp-relay counters ... 496
show ip dhcp-relay interface ... 496
show ip dhcp-snooping ... 497
show ip dhcp-snooping vlan ... 497
show ip dhcp-snooping binding ... 497
show ip ipfix ... 498
show ip mroute interface|next-hop|route|static-source-group ... 498
show ip verify source ... 499
show ip source binding ... 500
show interface FastEthernet|GigabitEthernet|Loopback|vlan ... 500
show rmon ... 502
show spanning-tree config|port|status ... 502
show test ... 503
show sys-info ... 503
show trace file ... 504
show trace level ... 504
monitor mlt error collision ... 505
monitor mlt error main ... 505
monitor mlt stats interface main ... 505
monitor mlt stats interface utilization ... 506
monitor ports error collision ... 506
monitor ports error extended ... 506
monitor ports error main ... 507
monitor ports statistics interface extended ... 507
monitor ports statistics interface main ... 508
monitor ports statistics interface utilization ... 509

monitor ports statistics rmon 509
monitor ports statistics stp 510
show filter acg 510
show filter acl action 511
show filter acl ethernet 511
show filter acl ip 511
show filter acl protocol 512
show filter acl statistics 512
show filter act ethernet 512
show filter act ip 513
show mlt 513
show mlt error 513
show mlt error collision 514
show smlt 514
show ip rsmlt 514
show ist 515
show ist stat 515
show mlt stats 515
show interface vlan 516
show vlan advance 516
show ip arp interface 516
show vlan autolearn-mac 517
show vlan vid basic 517
show vlan vid fdb-entry 517
show vlan vid fdb-filter 518
show vlan vid fdb-static 518
show interfaces vlan ip 518
show vlan manual-edit-mac 519
show vlan members 519
show vlan static-mcastmac 519
show interface loopback 520
show ip arp 520
show ip forward-protocol udp 520
show ip global 521
show ip interface 521
show ip irdp 522
show ip ospf 522
show ip ospf accept 523
show ip ospf area 523
show ip ospf ase 524
show ip ospf authentication interface 524
show ip ospf default-cost 525
show ip ospf host-route 525
show ip ospf ifstats 525
show ip ospf int-auth 526
show ip ospf int-timers 526
show ip ospf interface 526

show ip ospf lsdb ... 527
show ip ospf neighbours interface ... 528
show ip ospf redistribute ... 528
show ip ospf stats ... 528
show ip ospf timer interface ... 529
show ipv6 global ... 529
show ipv6 address ip ... 530
show ipv6 route ... 530
show ipv6 neighbor ... 531
show ipv6 interface ... 531
show ipv6 nd-prefix [detail] ... 532
show ip prefix-list ... 532
show ip rip ... 532
show ip rip interface ... 533
show ip routing ... 533
show route-map ... 533
show ip route ... 534
show ip tcp ... 535
show lldp ... 535
show slpp ... 537
show ports stats dhcp-relay ... 537
show vlan nlb-mode ... 537
show snmp-server ... 538
show eapol ... 538
show access-policy ... 539
show nsna ... 539
show nsna client ... 539
show nsna nsnas ... 540
show nsna interface ... 540
show nsna phone-signature ... 541
show nsna vlan ... 541
show radius ... 541
show radius-server ... 542
show sys log host ... 542
show boot config ... 543
show boot config choice ... 544
show boot config cli ... 544
show boot config config ... 544
show boot config flags ... 544
show boot config host ... 545
show boot config info ... 545
show boot config master ... 545
show boot config net ... 546
show boot config sio ... 546
show boot config tz ... 546
show autotopology ... 546
show basic config ... 547

show interfaces GigabitEthernet interface 547
show link-flap-detect 547
show logging config 548
show logging file 548
show log filter 549
show running-config 549
show slot 549
show sys hash-calc mltindex ip dest-mac dest-ip src-mac src-ip src-port mlt 550
show sys hash-calc mltindex non-ip dest-mac src-mac src-port mlt 551
show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt 551
show sys hash-calc mltindex non-ip-mcast dest-mac vlan-id src-port mlt 552
show sys-info 553
show sys perf 553
show sys sw 554
show ip vrf 554
Chapter 20: Customer Service 557
Getting technical documentation 557
Getting product training 557
Getting help from a distributor or reseller 557
Getting technical support from the Avaya Web site 557
Index 559

Chapter 1: New in this release

The following sections detail what is new in *Avaya Ethernet Routing Switch 8300 Commands Reference — ACLI, NN46200-104* for Release 4.2.

Features on page 25

Features

See the following sections for information about changes that are feature related.

STP BPDU filtering

Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) filtering is a new feature for Release 4.2. With STP BPDU filtering, a network administrator can prevent unknown devices from influencing an existing spanning tree topology and from flooding the network with BPDUs. using the Avaya command line interface (ACLI).

For more information about Avaya command line interface (ACLI), STP BPDU filtering commands, see:

- spanning-tree bpdu-filtering on page 148
- no spanning-tree bpdu-filtering on page 148
- spanning-tree bpdu-filtering timeout on page 149
- no spanning-tree bpdu-filtering timeout on page 149
- default spanning-tree bpdu-filtering on page 150
- show spanning-tree bpdu-filtering on page 151

IP spoof detection

IP spoof detection is a new feature for Release 4.2. With IP spoof detection, you can block the external use of the switch IP address.

For more information about Avaya command line interface (ACLI), IP spoof detection commands, see:

- spoof-detect on page 259
- no spoof-detect on page 260
- show spoof-detect on page 260

IPFIX

Internet Protocol Flow Information eXport (IPFIX) is a new feature for Release 4.2. With IPFIX, you can monitor the flow of information to third party collectors.

For more information about Avaya command line interface (ACLI), IIPFIX commands, see:

- ip ipfix (global) on page 215
- no ip ipfix enable on page 216
- no ip ipfix collector on page 216
- no ip ipfix exporter-enable on page 217
- ip ipfix (port) on page 217
- no ip ipfix (port) on page 218
- clear ip ipfix stats on page 218
- show ip ipfix on page 498

DHCP snooping

Dynamic Host Configuration Protocol (DHCP) snooping is a new feature for Release 4.2. DHCP snooping provides network security by preventing DHCP spoofing.

For more information about Avaya command line interface (ACLI), DHCP snooping commands, see:

- default ip dhcp-snooping on page 171
- ip dhcp-snooping (global) on page 175
- ip dhcp-snooping (interface) on page 175
- ip dhcp-snooping vlan on page 176
- no ip dhcp-snooping on page 179
- no ip dhcp-snooping vlan on page 179
- show ip dhcp-snooping on page 497

- show ip dhcp-snooping vlan on page 497
- show ip dhcp-snooping binding on page 497

Dynamic ARP inspection

Dynamic Address Resolution Protocol (Dynamic ARP) inspection is a new feature for Release 4.2. With Dynamic ARP inspection, you can add security to a network by validating ARP packets in the network.

For more information about Avaya command line interface (ACLI), Dynamic ARP inspection commands, see:

- ip arp-inspection vlan on page 174
- ip arp-inspection on page 174
- no ip arp-inspection vlan on page 178
- show ip arp-inspection vlan on page 493
- show ip arp-inspection interface on page 493

IP Source Guard

IP Source Guard is a new feature for Release 4.2. With IP Source Guard, you can add security to a network by filtering invalid client IP addresses.

For more information about Avaya command line interface (ACLI), DHCP snooping commands, see:

- ip verify source interface on page 176
- no ip verify source interface on page 179
- show ip verify source on page 499

BGP Lite

Border Gateway Protocol (BGP) Lite is a new feature for Release 4.2. With BGP Lite, you can provide loop-free inter-domain routing within an autonomous system (AS).

For more information about Avaya command line interface (ACLI), BGP Lite commands, see BGP Lite commands on page 429.

IGMPv3 snoop

Release 4.2 supports Internet Group Management Protocol version 3 (IGMPv3). IGMPv3 supports the PIM Source Specific Multicast (SSM) protocol. For more information about Avaya command line interface (ACLI), IGMPv3 commands, see:

- ip igmp on page 350
- ip igmp ssm dynamic-learning on page 374
- no ip igmp ssm dynamic-learning on page 374
- default ip igmp ssm dynamic-learning on page 375
- ip igmp ssm group-range on page 375
- ip igmp ssm-map on page 375
- ip igmp ssm-map enable on page 376
- no ip igmp ssm-map enable on page 376
- no ip igmp ssm-map on page 376
- ip igmp ssm-map all on page 377
- no ip igmp ssm-map all on page 377
- ip igmp dynamic-downgrade-version on page 353
- no ip igmp dynamic-downgrade-version on page 354
- default ip igmp dynamic-downgrade-version on page 354
- ip igmp compatibility-mode on page 353
- no ip igmp compatibility-mode on page 353
- default ip igmp compatibility-mode on page 353
- show ip igmp ssm on page 493
- show ip igmp ssm-map on page 493

Other changes

See the following sections for information about changes that are not feature related.

Customer service

Customer service chapter is added to this document. This chapter describes the complete range of services and support that Avaya provides to its customers. For more information about Avaya support, see Customer Service on page 557.

Comments? infodev@avaya.com

Chapter 2: Introduction

This guide describes the individual ACLI commands available for the Ethernet Routing Switch 8300 Software Release 4.1. The guide lists each command, the complete syntax, and a functional description from the Avaya Command Line Interface (ACLI).

The Avaya* Ethernet Routing Switch 8300 is a flexible and multifunctional Layer 2 and Layer 3 switch that supports diverse network architectures and protocols. The Ethernet Routing Switch 8300 provides security and control features such as Extensible Authentication Protocol over LAN (EAPoL), Simple Network Management Protocol, Version 3 (SNMP3), and Secure Shell (SSH). The Ethernet Routing Switch 8300 provides quality of service (QoS) for a high number of attached devices and supports future network requirements for QoS for critical applications, such as Voice over IP (VoIP).

Navigation

- Utility management commands on page 33
- Boot config commands on page 61
- System management commands on page 103
- SNMP commands on page 121
- Ethernet port commands on page 133
- Security commands on page 165
- IP protocol commands on page 199
- Layer 2 and 3 operations commands on page 265
- Route filters commands on page 307
- Test and diagnostic commands on page 329
- Multicast services commands on page 347
- Quality of Service commands on page 391
- Web server commands on page 405
- PoE commands on page 407
- LACP commands on page 417
- BGP Lite commands on page 429
- Show commands on page 483

Chapter 3: Utility management commands

This chapter describes the ACLI utility management commands and their parameters.

Navigation

- attribute on page 34
- boot on page 35
- cd on page 36
- chkdisk on page 36
- clear on page 37
- copy on page 38
- cp on page 39
- date on page 39
- delete on page 40
- delete on page 40
- dir on page 40
- disable on page 41
- edit on page 41
- enable on page 42
- end on page 42
- exit on page 42
- format on page 43
- format-flash on page 43
- grep on page 43
- help on page 44
- history on page 44
- install on page 45
- logout on page 45

- mkdir on page 45
- more on page 46
- mv on page 46
- pcmcia-stop on page 47
- peer on page 47
- ping on page 48
- pwd on page 49
- reload on page 49
- rename on page 50
- rlogin on page 50
- rlogin-sessions on page 51
- rsh on page 51
- save on page 52
- show running-config on page 52
- source on page 53
- sys-action on page 53
- telnet on page 54
- telnet-access on page 54
- test in loopback on page 55
- test on page 55
- trace on page 56
- trace auto on page 57
- traceroute on page 58
- write memory on page 59

attribute

Use this command to modify the MS-DOS file attributes.

Syntax

`attribute` <*file*> <*attributes*>

Variable definitions

Use the following table for the attribute command.

Variable	Value
attributes	specifies the file attributes as {+|-|A|S|H|R}. The range of values is 1 to 1536 characters.
file	specifies the MS-DOS file name. The range is 1 to 99 characters.

Command mode

Privilege EXEC mode

boot

Use this command to boot the switch with an image and a configuration file.

The command options lets you specify the boot source (flash, PCMCIA card, or TFTP server) and file name. If you do not specify a device and file, the ACLI uses the software and configuration files on the primary boot device that is defined by the Boot Monitor **choice** command.

Important:

For the changes made to the Boot Monitor CLI to take effect, you must use the **save** command to save the changed configuration file and then reboot the switch.

Syntax

boot [-y|config|license|WORD<1-99>]

Variable definitions

Use the following table to help you use the **boot** command.

Variable	Value
WORD<1-99>	Software image device and file name in the format *[a.b.c.d:]<file>***| /pcmcia/<file>|/flash/<file>**
config	is the software configuration device and file name in the format *[a.b.c.d:]<file>***| /pcmcia/<file>| /flash/<file>** The file name, including the directory structure, can be up to 1024 characters.
license	This is the license file.
-y	Suppresses the confirmation message before the switch reboots. If you omit this

	parameter, the system prompts you to confirm the action before the switch reboots.

Command mode

Privilege EXEC mode

cd

Use this command to change the current file system directory path.

Syntax

cd <*dir*>

Variable definitions

Use the following table for cd command.

Variable	Value
dir	specifies a directory path name up to 1536 characters.

Command mode

Privilege EXEC mode

chkdisk

Use this command to run a check of the file system for inconsistencies.

Syntax

chkdsk <*device*> **[repair]**

Variable definitions

Use the following table for chkdisk command:

Variable	Value
device	is the device name, for example /flash | / pcmcia, up to 1536 characters.
repair	repairs the errors found.

Comments? infodev@avaya.com

Command mode

Privilege EXEC mode

clear

Use this command to clear statistics from counters, flush entries from a table, or end a Telnet session.

Syntax

`clear`

Variable definitions

Use the following table for the **`clear`** command.

Variable	Value
`filter`	Clears filter statistics from the switch counters.
`ip`	Clears ip information.
`lacp`	Clear link aggregation info for specific mlt.
`qos`	Clear QoS statistics from the switch counters.
`port-stats`	Clears port statistics from the switch counters.
`telnet`	Ends the specified Telnet session.

Use the following table that you use to enter after the **`clear`** command.

Variable	Value
filter acl statistics	Clears filter acl statistics.
arp vlan <vid>	Clears ARP VLAN entries from the ARP table, where *vid* is the VLAN ID. The valid values are 0 to 4000.
route vlan <vid>	*vid* is the VLAN ID. The valid values are 0 to 4000.
[<ports>]	*ports* specifies the ports for which you are entering the command in the form: portlist {slot/port[-slot/port][, ...]}.

link-aggregate <mlt-id>	Clears link aggregation info for specific mlt. *mlt-id* is a number between 1-31.
policy-stats <qos policy ID>	Clears qos policy stats. *qos policy ID* is a number between 1-128.

Command mode

Privilege EXEC mode

copy

Use this command to copy a file from one device to another. You can also use a wildcard pattern with this command.

Syntax

copy *<srcfile> <destfile>*

Variable definitions

Use the following table for the copy command:

Variable	value
srcfile	specifies the source device and file name of the file to be copied in one of the following formats: • [a.b.c.d:] <file> • /pcmcia/ <file> • /flash/ <file> The range of values is 1 to 1536 characters.
destfile	specifies the destination device and file name of the file that receives the copied file. The range of values is 1 to 99 characters.

Command mode

Privilege EXEC mode

Comments? infodev@avaya.com

cp

Use this command to copy a file from one device to another. This command can be used with a wildcard pattern.

Syntax

cp <*srcfile*> <*destfile*>

Variable definitions

Use the following table for cp command:

Variable	Value
srcfile	specifies the source device and file name of the file to be copied in one of the following formats: • [a.b.c.d:] <file> • /pcmcia/ <file> • /flash/ <file> The range of values is 1 to 1536 characters.
destfile	specifies the destination device and file name of the file that receives the copied file. The range of values is 1 to 99 characters.

Command mode

Privilege EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

date

Use this command to display the current date settings for the switch.

Syntax

`date`

Command mode

User EXEC mode Privileged EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

delete

Use this command to remove a file or directory. A wildcard pattern can be used with this command.

Important:

This command can also be entered as **del**. There is no change in syntax or functionality when using the abbreviated command.

Syntax

delete <*file*> **[-y]**

Variable definitions

Use the following table for delete command:

Variable	Value
file	specifies the device and file name in one of the following formats: • /pcmcia/ <file> • /flash/ <file> The range of values is 1 to 99 characters.
-y	specifies bypassing the confirmation prompt.

Command mode

Privilege EXEC mode

dir

Use this command to list the files in a directory in MS-DOS format.

When you execute the **dir** command with no specified device, it displays the contents of all flash devices. When you specify flash or PCMCIA, the **dir** command displays only the contents of that device.

Syntax

dir [<*WORD<1-1536>* **] [-l]**

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`dir`** command.

Variable	Value
WORD<1-1536>	specifies the directory path name.
`-l`	displays file details if you specify a path name.

Command mode

Privileged EXEC mode

disable

Use this command to exit the Privilege EXEC command mode and return to the User EXEC command mode.

Syntax

`disable`

Command mode

Privilege EXEC mode

edit

Use this command to modify the contents of a script file.

Syntax

`edit` <*file*>

Variable definitions

Use the following table for edit command.

Variable	Value
file	specifies the file name /flash|/pcmcia value range of 1 to 99.

Command mode

Privilege EXEC mode

enable

Use this command to change from the User EXEC command mode to the Privilege EXEC command mode. If access to the Privilege EXEC command mode is password protected, you must supply a password when executing this command.

Syntax

```
enable
```

Command mode

User EXEC mode

Next command mode

Privilege EXEC mode

end

Use this command to exit Global configuration mode and return to Privilege EXEC mode. The command is equivalent to pressing Ctrl+Z on the keyboard.

Syntax

```
end
```

Command mode

Global configuration mode

exit

Use this command from within User EXEC mode or Privileged EXEC mode to end a terminal session and log out of the switch. Use this command from within Interface configuration mode to return to Global configuration mode and from Global configuration mode to return to Privilege EXEC mode.

Syntax

```
exit
```

Command mode

User EXEC mode Privileged EXEC Global configuration Interface configuration

Comments? infodev@avaya.com

format

Use this command to format the specified device (flash, or PCMCIA card).

Syntax

`format` <*device*>

Variable definitions

Use the following table for the format command:

Variable	Value
device	specifies the device name /flash or /pcmcia that you want to format. The valid range is 1 to 1536.

Command mode

Privilege EXEC mode

format-flash

Use this command to format the switch's on-board flash device with an FTL and MS-DOS file system.

Syntax

`format-flash`

Command mode

Privilege EXEC mode

grep

Use this command to display all lines in a file that have one or more matching strings within the file.

Syntax

`grep` <*WORD 0-99*> <*WORD 1-1536*>

Variable definitions

Use the following table to help you use the **grep** command.

Variable	Value
WORD<0-99>	Specifies the character string to be matched. The values range from 0 to 99.
WORD<1-1536>	Specifies the file name in one of the following formats: • /pcmcia/ <file> • /flash/ <file> The file name, including the directory structure, can be up to 1536 characters

Command mode

Privilege EXEC mode

help

Use this command to display a description of the interactive help system.

Syntax

`help`

Command mode

User EXEC Privilege EXEC mode Global configuration mode Interface configuration mode

history

Use this command to list the commands that you have entered during the current session.

Syntax

`history`

Command mode

Privilege EXEC mode

install

Use this command to start the Ethernet Routing Switch 8300 setup utility and set up the initial configuration to be effective at boot time.

Syntax

```
install
```

Command mode

Privilege EXEC mode

logout

Use this command to log out of the current ACLI, Telnet, or rLogin session from any mode, and return to the main console menu.

Syntax

```
logout
```

Command mode

User EXEC mode Privilege EXEC mode Global configuration mode Interface configuration mode

mkdir

Use this command to create a directory.

Syntax

`mkdir` <*dir*>

Variable definitions

Use the following table for mkdir command.

Variable	Value
dir	specifies the directory name with a value range of 1 to 99 characters.

Command mode

Privileged EXEC mode

more

Use this command to display the contents of a file one page at a time.

Syntax

`more [WORD<1-99>]`

Variable definitions

Use the following table to help you use the **`more`** command.

Variable	Value
`WORD <1-99>`	Specifies the filename in one of the following formats: • a.b.c.d:<file> • /pcmcia/ <file> • /flash/ <file> • /flash1/ <file> Values range from 1 to 99.

Command mode

Privilege EXEC mode

mv

Use this command to move or rename a file or directory. This command can be used with a wildcard pattern. You cannot use the mv command to move a file between two devices. Use the cp or the copy command instead.

Syntax

`mv` <*old_filename*> <*new_filename*>

Variable definitions

Use the following table for mv command.

Variable	Value

Comments? infodev@avaya.com

old_filename	specifies the old device and file name in one of the following formats: • /pcmcia/ <file> • /flash/ <file> The range of values is 1 to 1536 characters.
new_filename	specifies the new file name. The range of values is 1 to 99 characters.

Command mode

Privilege EXEC mode

pcmcia-stop

This command enables you to terminate access to the PCMCIA card.

Syntax

`pcmcia-stop`

Command mode

Privilege EXEC mode

peer

Use this command to access the standby CPU with telnet or rlogin. This command can make changes to the standby CPU without reconnecting to the console port on that module.

Syntax

`peer` <*operation*>

Variable definitions

Use the following table for peer command.

Variable	Value
operation	specifies the type of session access. The options are telnet or rlogin.

	Important: You must set an rlogin access policy on the standby CPU before you can use the rlogin peer command to access the standby from the master CPU. To set an access policy on the standby CPU, connect a terminal to the Console port on the standby CPU.

Command mode

Privileged EXEC mode

ping

Use this command to test the network connection to another network device. The **ping** command sends an Internet Control Message Protocol (ICMP) packet or echo message from the switch to the target device. If the device receives the packet, it sends a ping reply. When the switch receives the reply, it displays a message indicating that the specified IP address is alive. If no reply is received, a message indicates that the address is not responding.

Syntax

ping <*ipaddr*>

Variable definitions

Use the following table to help you use the **ping** command.

Variable	Value
ipaddr	is the IP address of the other network device.
datasize <*value*>	Specifies the size of the ping data. The range of *value* is 16 to 4076 bytes.
count <*value*>	Specifies the number of times to ping. The range of *value* is 1 to 9999, with a default of 1.
[-s]	Specifies a continuous ping (with an interval of -**I**)
[-I <*value*> **]**	Specifies the interval between transmissions in seconds. The range of *value* is 1 to 60.
[-t <*value*> **]**	Specifies the no-answer timeout value in seconds. The range of *value* is 1 to 120.

[-d]	Sets ping debug mode. In debug mode, the ping reply includes additional information about the device pinged.
scopeid <value>	Specifies the scope id. The range of *value* is 1 to 9999.
vrf <WORD 0-16>	Specifies the vrf name in the range of 0 to 16 characters.

Command mode

Privileged EXEC mode

pwd

Use this command to print the current working directory path in the file system.

Syntax

pwd

Command mode

Privilege EXEC mode

reload

Use this command to reset the switch. When you reset the switch, the most recently saved configuration file is used to reload the system parameters.

Syntax

reload [-y]

Variable definitions

Use the following table for reload command.

Variable	Value
-y	skips the information prompt. If you omit this option, the system prompts you to confirm the action before the switch performs the reload.

Command mode

Privilege EXEC mode

rename

Use this command to move or rename a file or directory. This command can be used with a wildcard pattern.

Syntax

`rename` <*old*> <*new*>

Variable definitions

Use the following table for rename command.

Variable	Value
old	specifies the old device and file name in one of the following formats: • /pcmcia/ <file> • /flash/ <file> The range of values is 1 to 1536 characters.
new	specifies the new device and file name. The range of values is 1 to 99 characters.

Command mode

Privilege EXEC mode

rlogin

Use this command to allow the login of a remote device.

Syntax

`rlogin` <*ipaddr*>

Variable definitions

Use the following table for rlogin command.

Variable	Value
ipaddr	specifies the IP address of the remote device in the format a.b.c.d.

Command mode

Privilege EXEC mode

rlogin-sessions

Use this command to specify the number of rlogin sessions.

Syntax

`rlogin-sessions` <*session*>

Variable definitions

Use the following table for rlogin-sessions command.

Variable	Value
sessions	specifies the number of rlogin sessions. The valid values are 0 to 8.

Command mode

Global configuration mode

rsh

Use this command to execute a shell command on a remote device.

Syntax

`rsh` <*ipaddr*> **`-l`** <*value*> <*cmd*>

Variable definitions

Use the following table to help you use the **`rsh`** command.

Variable	Value
ipaddr	specifies the IP address of the remote device in the format a.b.c.d
value	specifies the user login name. The range of values is a string of 0 to 1536 characters.
cmd	specifies the command to execute on the remote host. The range of values is a string of 1 to 1536 characters.

Command mode

Privilege EXEC mode

save

Use this command to save the running configuration to a selected file.

Syntax

save <*savetype*> **[file** <*value*> **][standby** <*value*> **] [backup** <*value*> **]**

Variable definitions

Use the following table for the save command.

Variable	Value
savetype	Specifies the type of file to save; options are config, bootconfig, log, and trace
file <*value*>	Specifies the file name in one of the following formats: • [a.b.c.d:] <file> • /pcmcia/ <file> • /flash/ <file> The file name, including the directory structure, can be up to 99 characters.
standby <*value*>	saves the specified file name to the standby CPU.
backup <*value*>	saves the specified file name and identifies the file as a backup file.

Command mode

Privileged EXEC mode

show running-config

Use this command to display the running system information.

Syntax

`show running-config`

Comments? infodev@avaya.com

Command mode

Privilege EXEC mode

source

Use this command to merge a configuration script file into the running configuration without having to reboot the switch.

Syntax

source <*file*>

Variable definitions

Use the following table for the source command.

Variable	Value
WORD <1-99>	Specifies the device and file name of the new configuration file in one of the following formats: • [a.b.c.d:] <file> • /pcmcia/ <file> • /flash/ <file> The range of values is 1 to 99 characters.
[debug]	Provides a debug script output.
[stop]	Stops the script when it finds an error in the file.
[syntax]	Verifies the script's syntax.

Command mode

Privileged EXEC mode

sys-action

This command resets system functions.

Syntax

sys-action

Variable definitions

Use the following table for the sys-action command.

Variable	Value
`cpuswitchover`	Resets the switch to change over to the backup CPU.
`resetconsole`	Reinitializes the hardware Universal Asynchronous Receiver/Transmitter (UART) drivers. Use this command only if the console connection is hung.
`resetcounters`	Resets all the statistics counters in the switch to zero.

Command mode

Privilege EXEC mode

telnet

Use this command to set up a Telnet session to a remote device, for example, to the standby CPU.

Syntax

`telnet [` <*ipaddr*> **`]`**

Variable definitions

Use the following table for the telnet command.

Variable	Value
ipaddr	is an optional parameter that specifies the IP address {a.b.c.d} of the remote device.

Command mode

Privilege EXEC mode

telnet-access

Use this command to set the number of seconds to wait for a Telnet login before closing the connection or to change the allowable number of inbound Telnet sessions.

Syntax

`telnet-access {login-timeout` <*seconds*> **`|sessions`** <*sessions*> **`}`**

Variable definitions

Use the following table for the telnet-access command.

Variable	Value
seconds	is the number of seconds to wait for a Telnet login before closing the connection. The valid range is 30 to 65535 seconds.
sessions	is the number of inbound Telnet sessions that you can have. The valid range is 0 to 8 sessions.

Command mode

Global configuration mode

test in loopback

Use this command to perform a loopback test or to stop a currently running loopback test.

Syntax

`test {loopback` <*slot/port*> **`|stop}`**

Variable definitions

Use the following table for the test command.

Variable	Value
slot/port	specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.

Command mode

Privilege EXEC mode

test

Use this command to set all interfaces or the specified interface(s) in testing mode.

Syntax

`test [port` <*slot/port*> **`]`**

Variable definitions

Use the following table for the test command.

Variable	Value
slot/port	specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.

Command mode

Interface configuration mode

trace

Use this command to display the status of the switch at any given time.

Syntax

`trace`

Variable definitions

Use the following table to help you use the **`trace`** command.

Variable	Value
`auto`	Automatic trace enable feature configuration commands.
`clear`	Clears the trace file.
`filter`	Filters trace messages.
`grep`	Performs a comparison of trace messages
`ipv6`	Configures IPv6 trace parameters.
`level` <*modid*> **`[`** <*level*> **`]`**	Displays the trace level on a software module for the specified module ID when the optional *level* parameter is omitted. The optional *level* parameter specifies trace levels. • 0 = Disabled • 1 = Very terse • 2 = Terse

Comments? infodev@avaya.com

	• 3 = Verbose • 4 = Very verbose
`off`	Disables tracing on a module.
`route-policy`	Traces a route policy.
`screen [` <*setting*> **`]`**	Enables or disables displaying the trace file. The *setting* value is either **`on`** or **`off`**.
`slot`	Specifies the line card slot number, from 1 to 10.

Command mode

Privileged EXEC mode

trace auto

Use this command to configure the switch to automatically enable a trace in the event CPU utilization reaches a pre-defined value.

Syntax

`trace auto`

Variable definitions

Use the following table for the **`trace auto`** command.

Variable	Value
`high-percentage` <*percent*>	Specifies the CPU utilization percentage above which auto trace must be enabled. *percent* is a value from 60 to 100. The default is 90.
`high-track-duration` <*seconds*>	Specifies the time in seconds to monitor CPU utilization before triggering a trace. *seconds* is a value from 3 to 10. The default is 5.
`low-percentage` <*percent*>	Specifies the CPU utilization percentage below which auto-trace should be disabled. *percent* is a value from 50 to 90. The default is 75.

low-track-duration <*seconds*>	Specifies the time, in seconds, to monitor CPU utilization before disabling the trace. *seconds* is a value from 3 to 10. The default is 5.
module <*modid*> <*level*>	Adds a module to be traced by the trace auto-enable feature. • *modid* identifies the module that you want to add. For example, 3 = Port Manager, 20 = Topology Discovery. The valid range is 0 to 66. For a list of valid module IDs, enter **trace level ?**. • *level* identifies the level of detail you want in the trace. For example, 0 = Disabled, 1 = Very Terse. The valid range is 0 to 7.

Command mode

Privileged EXEC mode

traceroute

Use this command to trace the route to a remote host. traceroute is a valuable tool for troubleshooting because it shows all the routes that are used or indicates that the remote network cannot be reached.

Syntax

traceroute <*ipaddr*> **[** <*datasize*> **] [-m** <*value*> **] [-p** <*value*> **] [-q** <*value*> **] [-w** <*value*> **] [-v]**

Variable definitions

Use the following table for the traceroute command.

Variable	Value
ipaddr	is the IP address {a.b.c.d} of the remote host.
datasize	is the size of the probe packet (1 to 1464).
-m<*value*>	is maximum time-to-live (TTL) value (1 to 255).
-p <*value*>	is the base UDP port number (0 to 65535).
-q <*value*>	is the number of probes per TTL (1 to 255).

-w <*value*>	is the wait time per probe (1 to 255).
-v	is the verbose mode (showing all).

Command mode

Privilege EXEC mode

write memory

Use this command to save the running configuration to memory.

Syntax

`write memory`

Command mode

Privilege EXEC mode

Comments? infodev@avaya.com

Chapter 4: Boot config commands

This chapter describes Avaya Command Line Interface (ACLI) boot configuration commands and their parameters.

Navigation

- boot choice license-file on page 64
- boot config bootp on page 64
- boot config choice config-file on page 65
- boot config choice image-file on page 65
- boot config cli more on page 66
- no boot config cli more on page 66
- boot config cli prompt on page 67
- boot config cli rlogin-sessions on page 67
- boot config cli screenlines on page 68
- boot config cli telnet-sessions on page 68
- boot config cli timeout on page 69
- boot config delay on page 69
- boot config flags on page 70
- no boot config flags on page 72
- boot config flags autoboot on page 73
- no boot config flags autoboot on page 74
- boot config flags block-snmp on page 74
- no boot config flags block-snmp on page 74
- boot config flags daylight-saving-time on page 74
- no boot config flags daylight-saving-time on page 75
- boot config flags debug-config on page 75
- no boot config flags debug-config on page 75

- boot config flags debugmode on page 76
- no boot config flags debugmode on page 76
- boot config flags factorydefaults on page 76
- no boot config flags factorydefaults on page 77
- boot config flags ftpd on page 77
- no boot config flags ftpd on page 77
- boot config flags info on page 78
- boot config flags logging on page 78
- no boot config flags logging on page 78
- boot config flags nncli on page 78
- no boot config flags nncli on page 79
- boot config flags reboot on page 79
- no boot config flags reboot on page 79
- boot config flags rlogind on page 80
- no boot config flags rlogind on page 80
- boot config flags savetostandby on page 80
- no boot config flags savetostandby on page 81
- boot config flags telnetd on page 81
- no boot config flags telnetd on page 81
- boot config flags tftpd on page 81
- no boot config flags tftpd on page 82
- boot config flags trace-logging on page 82
- no boot config flags trace-logging on page 82
- boot config flags verify-config on page 83
- no boot config flags verify-config on page 83
- boot config flags wdt on page 83
- no boot config flags wdt on page 84
- boot config host ftp-debug on page 84
- no boot config host ftp-debug on page 84
- boot config host password on page 85
- boot config host tftp-debug on page 85
- no boot config host tftp-debug on page 86

- boot config host tftp-hash on page 86
- no boot config host tftp-hash on page 86
- boot config host tftp-rexmit on page 87
- boot config host tftp-timeout on page 87
- boot config host user on page 88
- boot config master on page 88
- boot config net autonegotiate on page 89
- no boot config net autonegotiate on page 89
- boot config net bootp on page 90
- no boot config net bootp on page 90
- boot config net fullduplex on page 91
- no boot config net fullduplex on page 91
- boot config net ip on page 92
- boot config net restart on page 93
- boot net route on page 93
- boot config net speed on page 94
- boot config net tftp on page 95
- boot config sio on page 95
- boot config sio 8databits on page 96
- no boot config sio 8databits on page 96
- boot config sio baud on page 97
- boot config sio disable on page 97
- boo tconfig sio enable on page 97
- boot config sio info on page 98
- boot config sio mode on page 98
- boot config sio mtu on page 98
- boot config sio my-ip on page 99
- boot config sio pppfile on page 100
- boot config sio restart on page 100
- boot config sio slip-compression on page 101
- no boot config sio slip-compression on page 101

- boot config sio slip-rx-compression on page 101
- no boot config sio slip-rx-compression on page 102

boot choice license-file

This command loads the license file to the chassis.

Syntax

`boot choice <boot choice> license-file <file>`

Variable definitions

Use the following table for the boot choice license-file command.

Variable	Value
choice<*boot choice*>	Specifies the order in which the specified boot path is accessed when the switch is rebooted: primary, secondary, or tertiary.
license-file <*file*>	The source can be Flash memory, a PCMCIA card, or a remote TFTP server. • /flash/<file_name> • /pcmcia/<file_name> • <a.b.c.d.>:<file_name>

Command mode

Global configuration mode

boot config bootp

Use this command to set or clear the bootp CLI configuration commands.

Syntax

`boot config bootp`

Variable definitions

Use the following table for the **`boot config bootp`** command.

Variable	Value
image-name <*name*> [<*slot*>]	Set or clear the bootp CLI configuration commands.

Comments? infodev@avaya.com

Variable	Value
	• *name* is the bootfile to set or clear. If the name is set as default, then the configuration will be cleared. • *slot* is slot number to use for the bootfile. Acceptable values range from 1 to 10.

Command mode

Global configuration mode

boot config choice config-file

Use this command to select runtime and boot configuration file choices or change the order in which the boot sources (flash and PCMCIA card) are accessed.

Syntax

`boot config choice` <*boot-choice*> **`config-file`** <*file*>

Variable definitions

Use the following table for the **`boot config choice config-file`** command.

Variable	Value
<*boot-choice*>	Specifies the order in which the selected boot device is accessed when you reboot the switch. The options are: primary, secondary, and tertiary. The default order is to access the PCMCIA card first, and then the onboard flash.
config-file <*file*>	Specifies the boot configuration device and file name. The range of values is up to 256 characters including the path.

Command mode

Global configuration mode

boot config choice image-file

Use this command to select runtime and boot image file choices or change the order in which the boot sources (flash and PCMCIA card) are accessed.

Syntax

`boot config choice` <*boot-choice*> **`image-file`** <*file*>

Variable definitions

Use the following table to help you use the **`boot config choice`** command.

Variable	Value
<*boot-choice*>	Specifies the order in which the selected boot device is accessed when you reboot the switch. The options are: primary, secondary, and tertiary. The default order is to access the PCMCIA card first, and then the onboard flash.
file <*file*>	Specifies the boot image device and file name. The range of values is up to 256 characters including the path.

Command mode

Global configuration mode

boot config cli more

Use this command to set the output display for the Command Line Interface (CLI) to one line at a time.

Syntax

```
boot config cli more
```

Command mode

Global configuration mode

no boot config cli more

Use this command to set the output display for the Boot Monitor Command Line Interface (CLI) to continuous scrolling.

Syntax

```
no boot config cli more
```

Command mode

Global configuration mode

boot config cli prompt

Use this command to change the Boot Monitor prompt for the Command Line Interface (CLI) to the defined string.

Syntax

`boot config cli prompt` <*value*>

Variable definitions

Use the following table for the **`bootconfig cli prompt`** command.

Variable	Value
value	specifies the prompt text. The range of values is an ASCII string of 1 to 32 characters. **Important:** Enclose the string in quotation marks if it has spaces between characters.

Command mode

Global configuration mode

boot config cli rlogin-sessions

Use this command to specify the allowable number of inbound remote login sessions to the Boot Monitor Command Line Interface (CLI).

Syntax

`boot config cli rlogin-sessions` <*value*>

Variable definitions

Use the following table for the **`boot config cli rlogin-sessions`** command.

Variable	Value
<*value*>	specifies the allowable number of remote login sessions. The range of values is 0 to 8. The default is 8.

Command mode

Global configuration mode

boot config cli screenlines

Use this command to specify the number of lines in the output display for the Boot Monitor Command Line Interface (CLI).

Syntax

`boot config cli screenlines` <*value*>

Variable definitions

Use the following table for the**`boot config cli screenlines`** command.

Variable	Value
<*value*>	specifies the number of lines in the output display. The range of values is 1 to 64. The default is 23.

Command mode

Global configuration mode

boot config cli telnet-sessions

Use this command to specify the allowable number of inbound telnet sessions to the Boot Monitor Command Line Interface (CLI).

Syntax

`boot config cli telnet-sessions` <*value*>

Variable definitions

Use the following table for the **`boot config cli telnet-sessions`** command.

Variable	Value
<*value*>	specifies the allowable number of telnet sessions. The range of values is 0 to 8. The default is 8.

Command mode

Global configuration mode

boot config cli timeout

Use this command to specify the idle timeout period before automatic logout for Command Line Interface (CLI) sessions.

Syntax

`boot config cli timeout` <*seconds*>

Variable definitions

Use the following table for the **`boot config cli timeout`** command.

Variable	Value
<*seconds*>	specifies the timeout period in seconds. The range of values is 0 to 65536.

Command mode

Global configuration mode

boot config delay

Use this command to set the number of seconds a standby CPU should wait (delay) before trying to become the master CPU for booting the switch. This command applies only during a cold start and does not apply to a failover start.

Syntax

`boot config delay` <*seconds*>

Variable definitions

Use the following table for the **`boot config delay`** command.

Variable	Value
<*seconds*>	specifies the number of seconds of delay. The default range is 0-255 seconds.

Command mode

Global configuration mode

boot config flags

Use this command to set system flags. You enable or disable access services by setting flags. Changes to certain flags (factorydefaults, ftpd, tftpd, wdt) take effect only after you save changes to the boot configuration file and reset the switch.

Syntax

```
boot config flags
```

Variable definitions

Use the following table for the **`boot config flags`** command.

Variable	Value
autoboot	Sets the switch to automatically run the run-time image after being reset. Setting to no autoboot is useful for some debugging tasks. The default is autoboot.
block-snmp	Blocks access to the SNMP protocol. The default is no blocking.
daylight-saving-time	Enables Daylight Saving Time on the switch. The default is disabled.
debug-config	Enables run-time debugging of the configuration file. The default is no run-time debugging.
debugmode	Stops switch in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. A list of options is displayed that allows you to select a software module to debug. The default is no debugmode.
factorydefaults	Sets the runtime switch configuration to factory default settings. The default is to reset.
ftpd	Enables FTP server on the switch. To enable FTP, make sure the no bootconfig flags tftpd command is set. The default is no FTP.
jumboframe	Enables jumbo frames. The default is no jumbo frames.

Comments? infodev@avaya.com

Variable	Value
logging	Enables system logging to a file on the PCMCIA card. The default is system logging.
nocheck-sw-version	Disables the software version check.
nncli	Enables ACLI services on a switch. **Important:** Ethernet Routing Switch Command Line Interface (CLI) services are provided when ACLI is disabled.
reboot	Enables the automatic reboot on a fatal error. The default is to reboot. This command is equivalent to the debugmode command.
rlogind	Enables the rlogin/rsh server. The default is disabled.
savetostandby	Saves the config/bootconfig setup to a standby CPU, if one is available. The default is disabled.
sshd	Enables the secure shell (SSH) daemon. the default is disabled.
telnetd	Enables the Telnet server. The default is disabled.
tftpd	Enables the TFTP server. The default is disabled.
v-mode	Enables v-mode.
trace-logging	Enables system tracing to a file on the PCMCIA card. The default is disabled.
verify-config	Enables syntax checking of the configuration file and prevents execution of the file if an error is found. The factory default configuration file is loaded instead. The default is enabled.
wdt	Enables the hardware watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. The default is enabled.

Command mode

Global configuration mode

no boot config flags

Use this command to set system flags. You enable or disable access services by setting flags. Changes to certain flags (factorydefaults, ftpd, tftpd, wdt) take effect only after you save changes to the boot configuration file and reset the switch.

Syntax

```
no boot config flags
```

Variable definitions

Use the following table to help you use the **`no boot config flags`** command.

Variable	Value
autoboot	Sets the switch to automatically stop at the monitor prompt after being reset. Setting to no autoboot is useful for some debugging tasks. The default is autoboot.
block-snmp	Unblocks access to the SNMP protocol. To use this command, disable SSH secure mode first.
daylight-saving-time	Disables Daylight Saving Time on the switch.
debugmode	Automatically reboots the switch following a fatal error. The default is no debugmode.
debug-config	Disables run-time debugging of the configuration file.
factorydefaults	Disables reset of the switch configuration to factory default settings.
ftpd	Disables FTP server on the switch.
jumboframe	Enables jumbo frames. The default is no jumbo frames.
logging	Disables system logging to a file on the PCMCIA card.
nncli	Disables ACLI services on a switch. **Important:** Ethernet Routing Switch Command Line Interface (CLI) services are provided when ACLI is disabled.

Comments? infodev@avaya.com

Variable	Value
reboot	Disables automatic reboot on fatal errors.
rlogind	Disables the rlogin/rsh server.
sshd	Enables the SSH daemon. The default is disabled.
savetostandby	Disables saving the config/bootconfig setup to a standby CPU, even if one is available.
telnetd	Disables the Telnet server.
tftpd	Disables the TFTP server.
trace-logging	Disables system tracing to a file on the PCMCIA card.
verify-config	Disables syntax checking of the configuration file. Execution of the file occurs even if an error is found.
wdt	Disables the hardware watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors.

Command mode

Global configuration mode

boot config flags autoboot

Use this command to set the switch to automatically run the run-time image after being reset. Setting to **`no autoboot`** is useful for some debugging tasks. The default is **`autoboot`**.

Syntax

```
boot config flags autoboot
```

Command mode

Global configuration mode

no boot config flags autoboot

Use this command to set the switch to automatically stop at the monitor prompt after being reset. Setting to **no autoboot** is useful for some debugging tasks. The default is **autoboot**.

Syntax

```
no boot config flags autoboot
```

Command mode

Global configuration mode

boot config flags block-snmp

Use this command to block switch access to the SNMP protocol. The default is no blocking.

Syntax

```
boot config flags block-snmp
```

Command mode

Global configuration mode

no boot config flags block-snmp

Use this command to allow switch access to the SNMP protocol. To use this command, disable Secure Shell (SSH) secure mode first. The default is no blocking.

Syntax

```
no boot config flags block-snmp
```

Command mode

Global configuration mode

boot config flags daylight-saving-time

Use this command to enable Daylight Savings Time on the switch. The default is disabled.

Syntax

```
boot config flags daylight-saving-time
```

Command mode

Global configuration mode

no boot config flags daylight-saving-time

Use this command to disable Daylight Savings Time on the switch. The default is disabled

Syntax

```
no boot config flags daylight-saving-time
```

Command mode

Global configuration mode

boot config flags debug-config

Use this command to enable run-time debugging of the configuration file. The default is no run-time debugging.

Syntax

```
boot config flags debug-config
```

Command mode

Global configuration mode

no boot config flags debug-config

Use this command to disable run-time debugging of the configuration file. The default is no run-time debugging.

Syntax

```
no boot config flags debug-config
```

Command mode

Global configuration mode

boot config flags debugmode

Use this command to stop the switch in debug mode following a fatal error. Debug mode provides information equivalent to the **trace** commands. A list of options is displayed that allows you to select a software module to debug. The default is no debug mode.

Syntax

```
boot config flags debugmode
```

Command mode

Global configuration mode

no boot config flags debugmode

Use this command to automatically reboot the switch following a fatal error. The default is no debug mode.

Syntax

```
no boot config flags debugmode
```

Command mode

Global configuration mode

boot config flags factorydefaults

Use this command to reset the runtime switch configuration to factory default settings. Changes to the factorydefaults flag take effect only after you save changes to the boot configuration file and reset the switch. The default is to reset.

Syntax

```
boot config flags factorydefaults
```

Command mode

Global configuration mode

no boot config flags factorydefaults

Use this command to disable reset of the switch boot configuration to factory default settings. Changes to the factorydefaults flag take effect only after you save changes to the boot configuration file and reset the switch. The default is to reset.

Syntax

```
no boot config flags factorydefaults
```

Command mode

Global configuration mode

boot config flags ftpd

Use this command to enable the FTP (File Transfer Protocol) server on the switch. To enable FTP, ensure that the **`no boot config flags tftpd`** command is set. Changes to the FTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no FTP.

Syntax

```
boot config flags ftpd
```

Command mode

Global configuration mode

no boot config flags ftpd

Use this command to disable the FTP (File Transfer Protocol) server on the switch. Changes to the FTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no FTP.

Syntax

```
no boot config flags ftpd
```

Command mode

Global configuration mode

boot config flags info

Use this command to display information about the current boot configuration flag settings.

Syntax

```
boot config flags info
```

Command mode

Global configuration mode

boot config flags logging

Use this command to enable system logging to a file on the PCMCIA card. The default is system logging.

Syntax

```
boot config flags logging
```

Command mode

Global configuration mode

no boot config flags logging

Use this command to disable system logging to a file on the PCMCIA card. The default is system logging.

Syntax

```
no boot config flags logging
```

Command mode

Global configuration mode

boot config flags nncli

Use this command to enable ACLI services on the switch.

Important:
Ethernet Routing Switch Command Line Interface (CLI) services are provided when ACLI is disabled.

Syntax

```
boot config flags nncli
```

Command mode

Global configuration mode

no boot config flags nncli

Use this command to disable ACLI services on the switch.

Important:
Ethernet Routing Switch Command Line Interface (CLI) services are provided when ACLI is disabled.

Syntax

```
no boot config flags nncli
```

Command mode

Global configuration mode

boot config flags reboot

Use this command to enable the automatic reboot on a fatal error. The default is to reboot.

Syntax

```
boot config flags reboot
```

Command mode

Global configuration mode

no boot config flags reboot

Use this command to disable the automatic reboot on a fatal error. The default is to reboot.

Syntax

```
no boot config flags reboot
```

Command mode

Global configuration mode

boot config flags rlogind

Use this command to enable the rlogin/rsh server. The default is disabled.

Syntax

```
boot config flags rlogind
```

Command mode

Global configuration mode

no boot config flags rlogind

Use this command to disable the rlogin/rsh server. The default is disabled.

Syntax

```
no boot config flags rlogind
```

Command mode

Global configuration mode

boot config flags savetostandby

Use this command to save the config/bootconfig setup to a standby CPU, if one is available. The default is disabled.

Syntax

```
boot config flags savetostandby
```

Command mode

Global configuration mode

no boot config flags savetostandby

Use this command to disable saving the config/bootconfig setup to a standby CPU, even if one is available. The default is disabled.

Syntax

```
no boot config flags savetostandby
```

Command mode

Global configuration mode

boot config flags telnetd

Use this command to enable the Telnet server. The default is disabled.

Syntax

```
boot config flags telnetd
```

Command mode

Global configuration mode

no boot config flags telnetd

Use this command to disable the Telnet server. The default is disabled.

Syntax

```
no boot config flags telnetd
```

Command mode

Global configuration mode

boot config flags tftpd

Use this command to enable the TFTP (Trivial File Transfer Protocol) server. To enable TFTP, ensure that the **`no boot config flags ftpd`** command is set. Changes to the TFTP flag

take effect only after you save changes to the boot configuration file and reset the switch. The default is no TFTP.

Syntax

```
boot config flags tftpd
```

Command mode

Global configuration mode

no boot config flags tftpd

Use this command to disable the TFTP (Trivial File Transfer Protocol) server. Changes to the TFTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no TFTP.

Syntax

```
no boot config flags tftpd
```

Command mode

Global configuration mode

boot config flags trace-logging

Use this command to enable system tracing to a file on the PCMCIA card. The default is disabled.

Syntax

```
boot config flags trace-logging
```

Command mode

Global configuration mode

no boot config flags trace-logging

Use this command to disable system tracing to a file on the PCMCIA card. The default is disabled.

Syntax

```
no boot config flags trace-logging
```

Command mode

Global configuration mode

boot config flags verify-config

Use this command to enable syntax checking of the configuration file and prevent execution of the file, if an error is found. The factory default configuration file is loaded instead. The default is disabled.

Syntax

```
boot config flags verify-config
```

Command mode

Global configuration mode

no boot config flags verify-config

Use this command to disable syntax checking of the configuration file. Execution of the file occurs, even if an error is found. The default is disabled.

Syntax

```
no boot config flags verify-config
```

Command mode

Global configuration mode

boot config flags wdt

Use this command to enable the watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. Changes to the wdt flag take effect only after you save changes to the boot configuration file and reset the switch. The default is enabled.

Syntax

```
boot config flags wdt
```

Command mode

Global configuration mode

no boot config flags wdt

Use this command to disable the watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. Changes to the wdt flag take effect only after you save changes to the boot configuration file and reset the switch. The default is enabled.

Syntax

```
no boot config flags wdt
```

Command mode

Global configuration mode

boot config host ftp-debug

Use this command to enable the debug mode for FTP/FTPd (File Transfer Protocol) transfers with the remote host login. If you enable debug mode, debug messages are displayed on the management console screen. The default is disabled.

Syntax

```
boot config host ftp-debug
```

Command mode

Global configuration mode

no boot config host ftp-debug

Use this command to disable the debug mode for FTP/FTPd (File Transfer Protocol) transfers with the remote host login. If you disable the debug mode, debug messages are not displayed on the management console screen. The default is disabled.

Syntax

```
no boot config host ftp-debug
```

Command mode

Global configuration mode

boot config host password

Use this command to set the password for FTP (File Transfer Protocol) transfers with the remote host. When this password is set, a login with the password is required to perform FTP transfers with the remote host.

Important:

This password must match the password for the FTP server, or FTP operation fails.

Syntax

`boot config host password` <*value*>

Variable definitions

Use the following table for the **`boot config host password`** command.

Variable	Value
<*value*>	specifies the password. The range of values is a string of up to 16 characters.

Command mode

Global configuration mode

boot config host tftp-debug

Use this command to enable the debug mode for TFTP (Trivial File Transfer Protocol) transfers with the remote host. If you enable the debug mode, debug messages are displayed on the management console screen. The default is disabled.

Syntax

```
boot config host tftp-debug
```

Command mode

Global configuration mode

no boot config host tftp-debug

Use this command to disable the debug mode for TFTP (Trivial File Transfer Protocol) transfers with the remote host. If you disable the debug mode, debug messages are not displayed on the management console screen. The default is disabled.

Syntax

```
no boot config host tftp-debug
```

Command mode

Global configuration mode

boot config host tftp-hash

Use this command to enable TFTP (Trivial File Transfer Protocol) hash bucket display for the remote host. The default is disabled.

Syntax

```
boot config host tftp-hash
```

Command mode

Global configuration mode

no boot config host tftp-hash

Use this command to disable TFTP (Trivial File Transfer Protocol) hash bucket display for the remote host. The default is disabled.

Syntax

```
no boot config host tftp-hash
```

Command mode

Global configuration mode

boot config host tftp-rexmit

Use this command to set the TFTP (Trivial File Transfer Protocol) retransmission timeout for remote host.

Syntax

```
boot config host tftp-rexmit <seconds>
```

Variable definitions

Use the following table for the **`boot config host tftp-rexmit`** command.

Variable	Value
seconds	specifies the retransmission timeout in seconds. The range of values is 1 to 2147483647.

Command mode

Global configuration mode

boot config host tftp-timeout

Use this command to set the TFTP (Trivial File Transfer Protocol) timeout for the remote host.

Syntax

`boot config host tftp-timeout` <*seconds*>

Variable definitions

Use the following table for the **`boot config host tftp-timeout`** command.

Variable	Value
seconds	specifies the timeout in seconds. The range of values is 1 to 2147483647.

Command mode

Global configuration mode

boot config host user

Use this command to set the remote host user login name.

Syntax

`boot config host` *<value>*

Variable definitions

Use the following table for the **`boot config host user`** command.

Variable	Value
value	specifies the remote user login name. The range of values is a string of up to 16 characters.

Command mode

Global configuration mode

boot config master

Use this command to specify which CPU becomes master when the switch is turned on. The master CPU performs a loopback test to test the switch fabric.

Syntax

`boot config master` *<cpu-slot>*

Variable definitions

Use the following table to help you use the **`boot config master`** command.

Variable	Value
<cpu-slot><cpu-slot>	specifies the module position for the master CPU. The options are slot 5 or slot 6. The default is slot 5.

Command mode

Global configuration mode

boot config net autonegotiate

Use this command to enable autonegotiation for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - enabled
- **cpu2cpu** - disabled

Syntax

boot config net <*cpu-net-port*> **autonegotiate**

Variable definitions

Use the following table for the **boot config net autonegotiate** command.

Variable	Value
<*cpu-net-port*>	specifies the CPU network port. The options are **mgmt**, **cpu2cpu**.

Command mode

Global configuration mode

no boot config net autonegotiate

Use this command to disable autonegotiation for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - enabled
- **cpu2cpu** - disabled

Syntax

no boot config net <*cpu-net-port*> **autonegotiate**

Variable definitions

Use the following table to help you use the **no boot config net** command.

Variable	Value
<*cpu-net-port*>	specifies the CPU network port. The options are: mgmt, cpu2cpu

Command mode

Global configuration mode

boot config net bootp

Use this command to enable the Bootstrap Protocol (Bootp) for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The default is enabled for all specified port types.

Syntax

`boot config net` <*cpu-net-port*> **`bootp`**

Variable definitions

Use the following table for the **`boot config net bootp`** command.

Variable	Value
<*cpu-net-port*>	specifies the CPU network port. The options are mgmt, cpu2cpu.

Command mode

Global configuration mode

no boot config net bootp

Use this command to disable the Bootstrap Protocol (Bootp) for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The default is enabled for all specified port types.

Syntax

`no boot config net` <*cpu-net-port*> **`bootp`**

Variable definitions

Use the following table for the **`no boot config net bootp`** command.

Variable	Value
<*cpu-net-port*>	specifies the CPU network port. The options are: mgmt, cpu2cpu

Command mode

Global configuration mode

boot config net fullduplex

Use this command to enable the full-duplex mode for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - disabled
- **cpu2cpu** - enabled

Important:

Use the **boot config net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

boot config net *<cpu-net-port>* **fullduplex**

Variable definitions

Use the following table for the **boot config net fullduplex** command.

Variable	Value
<cpu-net-port>	pecifies the CPU network port. The options are mgmt, cpu2cpu.

Command mode

Global configuration mode

no boot config net fullduplex

Use this command to disable the full-duplex mode for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - disabled
- **cpu2cpu** - enabled

Syntax

no boot config net *<cpu-net-port>* **fullduplex**

Variable definitions

Use the following table for the **no boot config net fullduplex** command.

Variable	Value
<*cpu-net-port*>	specifies the CPU network ports. The options are: mgmt, cpu2cpu.

Command mode

Global configuration mode

boot config net ip

Use this command to assign an IP address and network mask to the specified CPU network port device. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Important:

Use the **boot config net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

boot config net <*cpu-net-port*> **ip** <*ipaddr*> <*mask*> <*cpu-slot value*>

Variable definitions

Use the following table for the **boot config net ip** command.

Variable	Value
<*cpu-net-port*>	Specifies the CPU network port. The options are: mgmt, cpu2cpu.
<*ipaddr*> <*mask*>	Assigns an IP address or mask for the specified port. The options are: • *a.b.c.d/x* • *a.b.c.d/x.x.x.x* • default (The default is 0.0.0.0.)
<*cpu-slot value*>	Specifies the slot position of the 8393SF module. The options are slot 5 or slot 6. If you do not specify a slot number for the IP address, the IP address is assigned to the currently active management module.

Command mode

Global configuration mode

Comments? infodev@avaya.com

boot config net restart

Use this command to restart the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Important:

Use the **`boot config net mgmt ip <ipaddr> <mask>`** command to assign an IP address to the switch.

Syntax

`boot config net` <*cpu-net-port*> **`restart`**

Variable definitions

Use the following table for the **`boot config net restart`** command.

Variable	Value
<*cpu-net-port*>	specifies the CPU network port. The options are mgmt, cpu2cpu

Command mode

Global configuration mode

boot net route

Use this command to set a route for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Important:

Use the **`boot config net mgmt ip <ipaddr> <mask>`** command to assign an IP address to the switch.

Syntax

`boot net` <*cpu-net-port*> **`route [add|del|net]`** <*netaddr*> <*gateway*>

Variable definitions

Use the following table for the **`boot net route`** command.

Variable	Value
<*cpu-net-port*>	Specifies the CPU network port. The options are: mgmt, cpu2cpu.
[add|del|net]	Performs the selected action on the specified port: • Adds the specified route for the selected port. • Deletes the specified route for the selected port. • Changes the specified route for the selected port to a network route.
<*netaddr*>	Specifies the IP address of the destination network for the selected port.
<*gateway*>	Specifies the IP address of the gateway for the selected port.

Command mode

Global configuration mode

boot config net speed

Use this command to set the connection speed for the specified CPU network port. The three network ports are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Important:

Use the **`boot config net mgmt ip <ipaddr> <mask>`** command to assign an IP address to the switch.

Syntax

`boot config net` <*cpu-net-port*> **`speed`**

Variable definitions

Use the following table for the **`boot config net speed`** command.

Variable	Value
<*cpu-net-port*>	Specifies the CPU network port. The options are: mgmt, cpu2cpu.
<10|100>	Sets the connection speed to 10 Mb/s or 100 Mb/s. The defaults are:

Comments? infodev@avaya.com

Variable	Value
	• mgmt - 10 Mb/s • cpu2cpu - 100 Mb/s

Command mode

Global configuration mode

boot config net tftp

Use this command to specify a TFTP (Trivial File Transfer Protocol) server for the CPU network port. The three network ports are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Important:

Use the **`boot config net mgmt ip <ipaddr> <mask>`** command to assign an IP address to the switch.

Syntax

`boot config net` <*cpu-net-port*> **`tftp`** <*ipaddr*>

Variable definitions

Use the following table for the **`boot config net tftp`** command.

Variable	Value
<*cpu-net-port*>	Specifies the CPU network port. The options are: mgmt, cpu2cpu.
<*ipaddr*>	Specifies the IP address of the TFTP server in the format a.b.c.d.

Command mode

Global configuration mode

boot config sio

Use this command to configure the CPU serial input/output (sio) port devices.

Syntax

`boot config sio [8databits <true|false>] [baud` <*rate*> **`] [restart]`**

Variable definitions

Use the following table for the **`boot config sio`** command.

Variable	Value
[8databits <true|false>]	Specifies the data bits per byte that the software interprets. The options are: • true (8 data bits per byte) • false (7 data bits per byte) The default is false.
[baud <*rate*>]	Specifies the baud rate for the selected port. The default is 9600.
[restart]	Shuts down and reinitializes the specified CPU serial port.

Command mode

Global configuration mode

boot config sio 8databits

Use this command to specify that the software interprets eight data bits per byte for the selected CPU serial input/output (sio) port devices. The default is seven data bits per byte.

Syntax

```
boot config sio 8databits
```

Command mode

Global configuration mode

no boot config sio 8databits

Use this command to specify seven data bits per byte for the software to interpret for the CPU serial input/output (sio) port.

Syntax

```
no boot config sio 8databits
```

Command mode

Global configuration mode

boot config sio baud

Use this command to specify the baud rate for the selected CPU serial input/output (sio) port.

Syntax

`boot config sio baud` <*rate*>

Variable definitions

Use the folowing table for the **`boot config sio baud`** command.

Variable	Value
<*rate*>	Specifies the baud rate for the port. The default is 9600.

Command mode

Global configuration mode

boot config sio disable

Use this command to disable the selected CPU serial input/output (sio) port.

Syntax

`boot config sio disable`

Command mode

Global configuration mode

boo tconfig sio enable

Use this command to enable the selected CPU serial input/output (sio) port.

Syntax

`boot config sio enable`

Command mode

Global configuration mode

boot config sio info

Use this command to display configuration information about the specified CPU serial input/output (sio) port.

Syntax

```
boot config sio info
```

Command mode

Global configuration mode

boot config sio mode

Use this command to specify the communication mode the selected CPU serial input/output (sio) port device.

Syntax

```
boot config sio mode <ascii|slip|ppp>
```

Variable definitions

Use the following table for the **`boot config sio mode`** command.

Variable	Value
<ascii|slip|ppp>	Specifies the communication mode for the serial port. The default is ascii. To configure the Console port, set the mode to ascii. If you are configuring the Modem port, you can set the port to use the same SLIP or PPP communication mode as the modem.

Command mode

Global configuration mode

boot config sio mtu

Use this command to specify the size of the maximum transmission unit (mtu) for a point-to-point link with the selected CPU serial input/output (sio) port device.

Comments? infodev@avaya.com

Syntax

boot config sio mtu <*bytes*>

Variable definitions

Use the following table for the **boot config sio mtu** command.

Variable	Value
<*bytes*>	Specifies the mtu size in bytes. The range of values is 0 to 2048. The default is 0.

Command mode

Global configuration mode

boot config sio my-ip

Use this command to specify the near-end IP address on a point-to-point link with the selected CPU serial input/output (sio) port device.

Syntax

boot config sio my-ip <*ipaddr*>

Variable definitions

Use the following table for the **boot config sio my-ip** command.

Variable	Value
<*ipaddr*>	Specifies the near-end IP address on a point-to-point link. The default is 0.0.0.0.

Command mode

Global configuration mode

boot config sio peer-ip

Use this command to specify the peer IP address on a point-to-point link with the selected CPU serial input/output (sio) port device.

Syntax

boot config sio peer-ip <*ipaddr*>

Variable definitions

Use the following table for the **boot config sio peer-ip** command.

Variable	Value
<*ipaddr*>	Specifies the peer IP address on a point-to-point link. The default is 0.0.0.0.

Command mode

Global configuration mode

boot config sio pppfile

Use this command to specify which file to use for PPP initialization parameters for the selected CPU serial input/output (sio) port.

Syntax

boot config sio pppfile <*file*>

Variable definitions

Use the following table for the **boot config sio pppfile** command.

Variable	Value
<*file*>	Specifies which file to use for PPP initialization parameters. The options are: • a.b.c.d: <*file*> • /pcmcia/ <*file*> • /flash/ <*file*>

Command mode

Global configuration mode

boot config sio restart

Use this command to shut down and reinitialize the selected CPU serial input/output (sio) port.

Syntax

```
boot config sio restart
```


Comments? infodev@avaya.com

Command mode

Global configuration mode

boot config sio slip-compression

Use this command to enable TCP/IP header compression for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
boot config sio slip-compression
```

Command mode

Global configuration mode

no boot config sio slip-compression

Use this command to disable TCP/IP header compression for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
no boot config sio slip-compression
```

Command mode

Global configuration mode

boot config sio slip-rx-compression

Use this command to enable TCP/IP header compression on the receive packet for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
boot config sio slip-rx-compression
```

Command mode

Global configuration mode

no boot config sio slip-rx-compression

Use this command to disable TCP/IP header compression on the receive packet for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
no boot config sio slip-rx-compression
```

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 5: System management commands

This chapter describes the Avaya Command Line Interface (ACLI) system management commands and their parameters.

Navigation

- auto-recover-delay on page 104
- default auto-recover-delay on page 104
- no auto-recover-delay on page 105
- autotopology on page 105
- no autotopology on page 105
- banner on page 106
- no banner on page 106
- clock set on page 107
- clock-sync-time on page 107
- enable on page 108
- load-module on page 110
- logging on page 110
- loginprompt on page 111
- no loginprompt on page 112
- mgmt-virtual-ip on page 112
- no mgmt-virtual-ip on page 113
- monitor-stats on page 113
- more on page 114
- no more on page 114
- msg-control on page 114
- no msg-control on page 115
- mtu on page 115

- passwordprompt on page 115
- no passwordprompt on page 116
- portlock on page 116
- prompt on page 116
- rlogin-sessions on page 117
- screenlines on page 117
- shutdown on page 118
- no shutdown on page 118
- sys-action cpuswitchover on page 118
- sys-action resetconsole on page 119
- sys-action resetcounters on page 119
- udpsrc-by-vip on page 119
- no udpsrc-by-vip on page 120

auto-recover-delay

Use this command to configure the auto recovery delay timer for ports.

Syntax

auto-recover-delay<*5-3600*>

Variable definitions

Use the following table for the auto-recover-delay command.

Variable	Value
<5-3600>	is the auto recovery delay time in seconds. The default is 30.

Command mode

Global configuration mode

default auto-recover-delay

Use this command to set the auto recovery delay timer to default values.

Syntax

```
default auto-recover-delay
```

Command mode

Global configuration mode

no auto-recover-delay

Use this command set the auto recovery delay timer to default values.

Syntax

```
no auto-recovery-delay
```

Command mode

Global configuration mode

autotopology

Use this command to turn the topology feature on. The topology feature generates topology packets used by network management software. When this feature is off, the topology table is not generated. The default is on.

Syntax

```
autotopology
```

Command mode

Global configuration mode

no autotopology

Use this command to turn the topology feature off. The topology feature generates topology packets used by network management software. When this feature is off, the topology table is not generated. The default is on.

Syntax

```
no autotopology
```

Command mode

Global configuration mode

banner

Use this command to add lines of text to the ACLI login banner.

Syntax

banner <*string*>

Variable definitions

Use the following table for the banner command.

Variable	Value
string	specifies the lines of text. The range of values is an ASCII string of 1 to 1024 characters. **Important:** Enclose the string in quotation marks if it has spaces between characters.
custom	Enables the use of the custom banner as defined by `banner` <*banner*>.
motd [displaymotd |<motd>]	Enables the display of a Message of the Day (MoTD) following the user login. The MoTD is from 1- 1536 characters.
static	Enables the default Avaya banner.
<*banner*>	Enables the user of a custom banner defined by the user. The length is from 0- 80 characters.

Command mode

Global configuration mode

no banner

Use this command to disable the display of a banner following the user login.

Comments? infodev@avaya.com

Syntax

```
no banner <motd> [displaymotd]
```

Variable definitions

Use the following table for the no banner command.

Variable	Value
<*motd*>	specifies a message from 1- 1536 characters.

clock set

Use this command to set the calendar time in the form of hour, minute, second, month, day, and year. You set the time zone using the **`bootconfig tz`** command at the Global configuration level.

Syntax

`clock set` <*MMddyyyyhhmmss*>

Variable definitions

Use the following table for the clock set command.

Variable	Value
<*MMddyyyyhhmmss*>	sets the calendar time in the format month, day, year, hour, minutes, seconds. Note that you must be logged in as rwa to use this command.

Command mode

Global configuration mode

clock-sync-time

Use this command to configure the time interval between synchronizing the real-time and system clocks.

Syntax

`clock-sync-time` <*minutes*>

Variable definitions

Use the following table for the clock-sync-line command.

Variable	Value
minutes	pecifies the time interval between synchronizations. The range of values is 15 to 3600 minutes.

Command mode

Global configuration mode

enable

Use this command to change the current command mode from Privileged EXEC to Global Config, or, if you execute this command in Global Config mode, to change the password for the enable command.

Syntax

`enable`

In Global configuration mode, the syntax is:

`enable` <*password*>

Variable definitions

Use the following table for the enable command.

Variable	Value
password	string length is from 1-32 characters.

Command mode

Global configuration mode

link-flap-detect

Use this command to configure the control of link state changes.

Syntax

`link-flap-detect`

Comments? infodev@avaya.com

Variable definitions

Use the following table for the link-flap-detec command.

Variable	Value
auto-port-down	Enables automatic disabling of the port if the link-flap threshold is exceeded. The default is enable.
frequency <*frequency*>	Sets the number of changes that are allowed during the time specified by the interval command. The frequency range is 1–9999. The default is 10.
interval <*interval*>	Sets the link-flap-detect interval in seconds. The interval range is 2–600. The default is 60.
send-trap	Enables trap sending to force the port out of service. The default is enable.

Command mode

Global configuration mode

no link-flap-detect auto-port-down

Use this command to disable the automatic disabling of port.

Syntax

```
no link-flap-detect auto-port-down
```

Command mode

Global configuration mode

no link-flap-detect send-trap

Use this command to disable sending traps.

Syntax

```
no link-flap-detect send-trap
```

command mode

Global configuration mode

load-module

Use this command to dynamically load modules.

Syntax

```
load-module {<AES>|<3DES>|<DES>}
```

Variable definitions

Use the following table for the load-module command.

Variable	Value
<*filename*>	Sets the module ID to AES.
3DES<*filename*>	Sets the module ID to 3 DES.
DES<*filename*>	Sets the module ID to DES

Command mode

Global configuration mode

logging

Use this command to configure and display the log files for the switch. When you save the **`bootconfig flags logging`** command in the configuration file, the log entries are written to the **`/pcmcia/syslog.txt`** file. If the logging flag is not set to true, the entries are stored in memory.

Syntax

`logging [clear] [filter` <*string*> **`] [level <level>] [logToPCMCIA] [screen <true/false>] [transferFile`** <*hostID*> **`[`** <*add-ip*>|<*filename*>|<*remove-IP*> **`]] [write]`**

Variable definitions

Use the following table for the logging command

Variable	Value
[clear]	Erases log file entries.
[filter <*string*>]	Specifies a string to match in the log file.
[level <*level*>]	Shows and sets the logging level. level is one of the following values:

Comments? infodev@avaya.com

Variable	Value
	0 = Information; all messages are recorded. 1 = Warning; only warning and more serious messages are recorded. 2 = Error; only error and more serious messages are recorded. 3 = Manufacturing; this parameter is not available for customer use. 4 = Fatal; only fatal messages are recorded.
logToPCMCIA	Starts logging to PCMCIA media.
screen <true|false>	Enables (true) or disables (false) screen logging.
[transferFile <*hostID*> [<add-IP>| <filename> |<remove-IP>]]	Sets the remote host you wish to log, where: • *add-IP* and *remove-IP* specify the IP address. • *filename* is a string from 1- 256.
[write]	Writes an entry to the log file.

Command mode

Global configuration mode

loginprompt

Use this command to change the CLI login prompt.

Syntax

`loginprompt` <*string*>

Variable definitions

Use the following table for the loginprompt command.

Variable	Value
<*string*>	specifies the text for the new CLI login prompt. The range of values is an ASCII string of 1 to 1536 characters. **Important:** Enclose the string in quotation marks if it has spaces between characters.

Command mode

Privileged EXEC mode

no loginprompt

Use this command to disable the default login banner.

Syntax

```
no loginprompt
```

Command mode

Privilege EXEC mode

mgmt-virtual-ip

Use this command to create a virtual management address for the Ethernet Routing Switch 8300. Although each CPU can have its own unique physical IP address, they share a common virtual address. This is helpful when the master CPU fails and the standby CPU comes up. If the virtual IP address is defined, the switch still responds to this address, even when using the backup CPU.

Syntax

`mgmt-virtual-ip` <*ipaddr*> <*mask*>

Variable definitions

Use the following table for the mgmt-virtual-ip command.

Variable	Value
<*ipaddr*> <*mask*>	specifies the IP address and mask that you assign to the virtual management port **Important:** Ensure that the virtual IP address is on the same IP subnet as the CPU physical IP address(es).

Command mode

Global configuration mode

Comments? infodev@avaya.com

no mgmt-virtual-ip

Use this command to remove/delete the virtual management IP address.

Syntax

no mgmt-virtual-ip <*ipaddr*> <*mask*>

Variable definitions

Use the following table for the no mgmt-virtual-ip command.

Variable	Value
<*ipaddr*> <*mask*>	specifies the IP address and mask assigned to the virtual management port.

Command mode

Global configuration mode

monitor-stats

Use this command to configure and manage the monitor duration (refresh rate).

Syntax

monitor-stats [duration <*integer*> **] [interval** <*integer*> **]**

Variable definitions

Use the following table for the monitor-stats command.

Variable	Value
[duration <*integer*>]	Changes the monitoring time duration (refresh rate) for the monitor commands. duration <*integer*> specifies the time duration in seconds. The range of values is 1 to 1800. The default is 300.
[interval <*integer*>]	Changes the monitoring time interval between screen updates set by the monitor commands. interval <*integer*> specifies the time duration in seconds. The range of values is 1 to 600. The default is 5.

Command mode

Global configuration mode

more

Use this command to set the display output to scroll one page at a time.

Syntax

```
more
```

Command mode

Privilege EXEC mode

no more

Use this command to set the display output to continuous scrolling.

Syntax

```
no more
```

Command mode

Privilege EXEC mode

msg-control

Use this command to enable system message control and suppress duplicate error messages.

Syntax

```
msg-control
```

Command mode

Global configuration mode

no msg-control

Use this command to disable the system message control.

Syntax

```
no msg-control
```

Command mode

Global configuration mode

mtu

This command is not valid in the Ethernet Routing Switch 8300since Jumbo Frames are not supported in Release 2.2.

passwordprompt

Use this command to change the ACLI password prompt.

Syntax

`passwordprompt` <*string*>

Variable definitions

Use the following table for the passwordprompt command.

Variable	Value
<*string*>	specifies the text for the CLI password prompt. The range of values is an ASCII string of 1 to 1536 characters. **Important:** Enclose the string in quotation marks if it has spaces between characters.

Command mode

Privileged EXEC mode

no passwordprompt

Use this command to disable changing the ACLI password prompt.

Syntax

```
no passwordprompt
```

Command mode

Privilege EXEC mode

portlock

Use this command to globally turn port locking on or off. To specify the ports to be locked, use the **`ethernet <ports> lock`** command.

This command enables port locking globally so you can enable or disable per-port locking. Locking a port or ports prevents other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is first unlocked.

Syntax

```
portlock <on|off>
```

Command mode

Global configuration mode

prompt

Use this command to set the root-level prompt.

Syntax

`prompt` *<prompt>*

Variable definitions

Use the following table for the prompt command.

Variable	Value
<prompt>	specifies the text for the root-level prompt. The range of values is an ASCII string of 1 to

Comments? infodev@avaya.com

Variable	Value
	255 characters. The default prompt is Passport-8310

Command mode

Privilege EXEC mode

rlogin-sessions

Use this command to set the allowable number of inbound rlogin/rsh sessions.

Syntax

`rlogin-sessions` <*nsessions*>

Variable definitions

Use the following table for the rlogin-sessions command:

Variable	Value
<*nsessions*>	specifies the number of sessions. The range of values is 0 to 8. The default is 8.

Command mode

Global configuration mode

screenlines

Use this command to set the number of lines in the output display of the terminal screen.

Syntax

`screenlines` <*nlines*>

Variable definitions

Use the following table for the screenlines command.

Variable	Value
<*nlines*>	specifies the number of lines. The range of values is 8 to 64.

Command mode

Privileged EXEC mode

shutdown

Use this command to configure shutdown policies for a module.

Syntax

shutdown <*slots*>

Variable definitions

Use the following table for the shudown command:

Variable	Value
<*slots*>	specifies the applicable slot number in the chassis. The range of values is 1 to 10. **Important:** Slots are numbered from top to bottom in Ethernet Routing Switch 8300switches.

Command mode

Global configuration mode

no shutdown

Use this command to enable the administrative status of the module.

Syntax

no shutdown <*slots*>

Command mode

Global configuration mode

sys-action cpuswitchover

Use this command to reset the switch to changeover to the backup CPU.

Syntax

```
sys-action cpuswitchover
```

Command mode

Privileged EXEC mode

sys-action resetconsole

Use this command to reinitializes the hardware UART drivers. Use this command only if the console or modem connection is hung.

Syntax

```
sys-action resetconsole
```

Command mode

Privilege EXEC mode

sys-action resetcounters

Use this command to reset all the statistics counters in the switch to zero.

Syntax

```
sys-action resetcounters
```

Command mode

Privilege EXEC mode

udpsrc-by-vip

Use this command to enable the flag that directs the IP header to have the same source address as the management virtual IP address for self-generated User Datagram Protocol (UDP) packets.

Syntax

```
udpsrc-by-vip
```

Command mode

Global configuration mode

no udpsrc-by-vip

Use this command to disable the flag that directs the IP header to have the same source address as the management virtual IP address for self-generated User Datagram Protocol (UDP) packets.

Syntax

```
no udpsrc-by-vip
```

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 6: SNMP commands

This chapter describes ACLI SNMP commands and their parameters.

Navigation

- snmp-server authentication-trap on page 122
- no snmp-server authentication-trap on page 122
- snmp-server bootstrap on page 122
- snmp-server community on page 123
- snmp-server community name on page 123
- snmp-server community security on page 124
- no snmp-server community on page 124
- snmp-server contact on page 125
- snmp-server group on page 125
- no snmp-server group on page 126
- snmp-server host on page 126
- no snmp-server host on page 127
- snmp-server location on page 127
- snmp-server member on page 128
- no snmp-server member on page 128
- snmp-server name on page 129
- snmp-server user on page 130
- no snmp-server user on page 130
- snmp-server view on page 131
- no snmp-server view on page 132
- no snmp-server view on page 132

snmp-server authentication-trap

Use this command to specify authentication failure traps of SNMP transmission.

Syntax

```
snmp-server authentication-trap
```

Command mode

Global configuration mode

no snmp-server authentication-trap

Use this command to specify authentication failure traps of SNMP transmission.

Syntax

```
no snmp-server authentication-trap
```

Command mode

Global configuration mode

snmp-server bootstrap

Use this command to provide a configuration for switch access.

Syntax

```
snmp-server bootstrap
```

Variable definitions

Use the following table to help you use the **`snmp-server bootstrap`** command:

Variable	Value
`min-secure`	Provides the minimum security configuration for switch access.
`semi-secure`	Provides restricted view access to the switch.
`very-secure`	Does not provide any configuration to users; users must configure the switch by themselves.

Command mode

Global configuration mode

snmp-server community

Use this command to create and configure an SNMPv1/v2 community on the switch.

Syntax

```
snmp-server community
```

Variable definitions

Use the following table to help you use the **`snmp-server community`** command:

Variable	Value
<*comm Idx*>	A unique SNMP community index value. The range is 1-32 characters.
<*name*>	The community string input for the community table that represents a configuration. The range is 1-255 characters.
<*security*>	Maps the community string to the security name in VACM Group Member Table. The range is 1-32.

Command mode

Global configuration mode

snmp-server community name

Use this command to change the name of an SNMP community by changing the name of an entry in the SNMP community table.

Syntax

`snmp-server community name` <*comm Idx*> <*new-name*>

Variable definitions

Use the following table to help you use the **`snmp-server community name`** <*comm Idx*> <*new-name*> command:

Variable	Value
<*comm Idx*>	Specifies a unique SNMP community index value. The range is 1-32 characters.
<*new-name*>	Specifies the new name for the entry in the community table.

Command mode

Global configuration mode

snmp-server community security

Use this command to change the security name of an SNMP community by changing the security name of an entry in the SNMP community table.

Syntax

`snmp-server community security` <*comm Idx*> <*security*>

Variable definitions

Use the following table for the snmp-server community security command:

Variable	Value
<*comm Idx*>	Specifies a unique SNMP community index value. The range is 1-32 characters.
<*security*>	Maps the community string to the security name in VACM Group Member Table.

Command mode

Global configuration mode

no snmp-server community

Use this command to delete an SNMP community on the switch by deleting an entry in the SNMP community table.

Syntax

`no snmp-server community` <*comm Idx*>

Variable definitions

Use the following table to help you use the **`no snmp-server community`** <*comm Idx*> command:

Comments? infodev@avaya.com

Variable	Value
<*comm Idx*>	specifies a unique SNMP community index value. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

snmp-server contact

Use this command to set the SNMP contact information for the switch.

Syntax

`snmp-server contact` <*contact*>

Variable Defintion

Use the following table to help you use the **`snmp-server contact`** <*contact*> command:

Variable	Value
<*contact*>	specifies the contact information text. The range of values is an ASCII string from 0 to 255 characters (for example a phone extension or email address). Strings with spaces must be enclosed in quotes (e.g., "John Smith").

Command mode

Global configuration mode

snmp-server group

Use this command to create new access for a group in the VACM table.

Syntax

`snmp-server group` <*group name*> <*prefix*> <*model*> <*level*>

Variable definitions

Use the following table to help you use the **`snmp-server group`** <*group name*> <*prefix*> <*model*> <*level*> command:

Variable	Value
`view <group name> <prefix> <model> <level> [read <value>] [write <value>]`	Assigns a MIB view for the specified group. • **`read`** *value* indicates that you want the group to have read access to the specified value (that is, MIB view). • **`write`** *value* indicates that you want the group to have write access to the specified value (that is, MIB view).

Command mode

Global configuration mode

no snmp-server group

Use this command to delete group access from the v3 VACM table.

Syntax

`no snmp-server group` <*group name*> <*prefix*> <*model*> <*level*>

Variable definitions

Use the following table to help you use the **`no snmp-server group`** <*group name*> <*prefix*> <*model*> <*level*> command:

Variable	Value
`view <group name> <prefix> <model> <level> [read <value>] [write <value>]`	Assigns a MIB view for the specified group. • **`read`** *value* indicates that you want the group to have read access to the specified value (that is, MIB view). • **`write`** *value* indicates that you want the group to have write access to the specified value (that is, MIB view).

Command mode

Global configuration mode

snmp-server host

Use this command to set an SNMP trap receiver.

Comments? infodev@avaya.com

Syntax

snmp-server host <*ipaddr*> **<v1|v2c>** <*commstr*>

Variable definitions

Use the following table to help you use the **snmp-server host** <*ipaddr*> **<v1|v2c>** <*commstr*> command:

Variable	Value
<*ipaddr*>	Specifies the IP address of the trap receiver.
<v1|v2c>	Specifies SNMP version 1 or SNMP version 2.
<*commstr*>	Specifies the input community string from 1 to 20 characters.

Command mode

Global configuration mode

no snmp-server host

Use this command to delete the SNMP trap receiver.

Syntax

no snmp-server host <*ipaddr*>

Variable definitions

Use the following table to help you use the **no snmp-server host** <*ipaddr*> command:

Variable	Value
<*ipaddr*>	Specifies the IP address of the trap receiver.

Command mode

Global configuration mode

snmp-server location

Use this command to set the location information for the switch.

Syntax

snmp-server location <*location*>

Variable definitions

Use the following table to help you use the **snmp-server location** <*location*> command:

Variable	Value
<location>	Specifies the location information. The range of a values is an ASCII string from 0 to 255 characters (for example, Finance).

Command mode

Global configuration mode

snmp-server member

Use this command to create a new group member on the Ethernet Routing Switch 8300.

Syntax

snmp-server member <*user name*> <*model*> *[<group name>]*

Variable definitions

Use the following table to help you use the **snmp-server member** <*user name*> <*model*> *[<group name>]*

Variable	Value
name <*user name*>	Changes the group name for the v3 VACM table. Specifies the name of the user group. The range is 1 to 32 characters.
<*model*>	Specifies the message processing model to use when generating an SNMP message. The valid options are usm, snmpv1, and snmpv2c.
<*group name*>	Assigns the user to the group for data access. The range is 1 to 32 characters.

Command mode

Global configuration mode

no snmp-server member

Use this command to delete a user group from the v3 VACM table.

Comments? infodev@avaya.com

Syntax

`no snmp-server member` <*user name*> <*model*>

Variable definitions

Use the following table to help you use the **`no snmp-server member`** <*user name*> <*model*>

Variable	Value
<*user name.*	specifies the name of the user group. The range is 1 to 32 characters.
<*model*>	specifies the message processing model to use when generating an SNMP message. The valid options are usm, snmpv1, and snmpv2c.

Command mode

Global configuration mode

snmp-server name

Use this command to set the root-level prompt name for the switch.

Syntax

`snmp-server name <prompt>`

Variable definitions

Use the following table to help you use the **`snmp-server name <prompt>`**

Variable	Value
<prompt>	Specifies the text of the root-level prompt name for the SNMP server. The range of values is an ASCII string from 0 to 255 characters (for example, LabSC7 or Closet4).

Command mode

Global configuration mode

snmp-server user

Use this command to create a new user in the USM table on the Ethernet Routing Switch 8300.

Syntax

`snmp-server user` <*UserName*> *[*<*auth protocol*> **`] [auth`** <*password*> **`] [priv`** <*password*> **`]`**

Variable definitions

This command uses the following options:

Variable	Value
<*UserName*>	Specifies the SNMPv3 user name. The name is used as an index to the table. The range is 1 to 32 characters.
<*auth protocol*>	Specifies an authentication protocol. If no value is entered, the entry has no authentication capability. The protocol choices are MD5 and SHA.
<*auth password.*	Specifies an authentication password. If no value is entered, the entry has no authentication capability. The range is 1 to 32 characters.
priv <*password*>	Assigns a privacy password. If no value is entered, the entry has no privacy capability. The range is 1 to 32 characters. You must set authentication before you can set the privacy option.

Command mode

Global configuration mode

no snmp-server user

Use this command to delete a user from the v3 VACM table.

Syntax

`no snmp-server user` <*user name*>

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **no snmp-server user** <*user name*> command.

Variable	Value
<*user name*>	Specifies the user's security name that is an index to the table. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

snmp-server view

Use this command to create a new entry for the MIB View table on the Ethernet Routing Switch 8300.

Syntax

snmp-server view <*View Name*> <*subtree oid*> **[mask** <*value*> **] [type** <*value*> **]**

Variable definitions

Use the following table to help you use the **snmp-server view** <*View Name*> <*subtree oid*> **[mask** <*value*> **] [type** <*value*> **]**

Variable	Value
<*View Name*>	Represents an SNMP access view. The range is 1 to 32 characters.
<*subtree oid*>	The prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1 to 32 characters.
mask <*value*>	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
type <include|exclude>	Determines whether access to a mib object is granted or denied.

Command mode

Global configuration mode

no snmp-server view

Use this command to delete an entry for the MIB view table.

Syntax

`no snmp-server view` <*view name*> <*subtree oid*>

Variable definitions

Use the following table to help you use the

Variable	Value
<*view name*>	Specifies the group name of the user. The range of values is 1 to 32 characters.
<*subtree oid*>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 7: Ethernet port commands

This chapter describes ACLI Ethernet port commands and their parameters.

Navigation

- action on page 134
- auto-negotiate on page 135
- no auto-negotiate on page 135
- auto-recover-port on page 136
- default auto-recover-port on page 136
- no auto-recover-port on page 137
- bcast-mcast-rate-limit on page 137
- cp-limit on page 138
- no cp-limit on page 138
- default-vlan-id on page 139
- duplex on page 140
- eapol on page 140
- no eapol on page 142
- encapsulation on page 143
- no encapsulation on page 143
- linktrap on page 144
- no linktrap on page 144
- lock on page 145
- no lock on page 145
- name on page 146
- shutdown on page 146
- no shutdown on page 147
- boot config flags spanning-tree-mode on page 147
- no boot config flags spanning-tree-mode on page 148

- spanning-tree mstp on page 151
- show spanning-tree mstp config on page 152
- spanning-tree mstp cist on page 153
- no spanning-tree mstp cist on page 153
- spanning-tree mstp msti on page 154
- show spanning-tree mstp msti config on page 154
- spanning-tree mstp msti on page 155
- show spanning-tree mstp port on page 155
- show spanning-tree mstp status on page 156
- spanning-tree rstp on page 156
- no spanning-tree rstp on page 157
- show spanning-tree rstp config on page 157
- show spanning-tree rstp status on page 158
- spanning-tree rstp on port on page 158
- no spanning-tree rstp on port on page 159
- show spanning-tree rstp port on page 159
- tx-queue on page 160
- no tx-queue on page 160
- unknown-mac-discard on page 161
- no unknown-mac-discard on page 162
- test loopback on page 163
- test stop on page 163
- untagged-frames-discard on page 164
- no untagged-frames-discard on page 164

action

Use this command to perform port-specific actions such as flush table entries.

Syntax

```
action <port | none | flushMacFdb |flushALL| clearLoopDetectAlarm>
```

Variable definitions

Use the following table to help you use the **`action <port | none | flushMacFdb | flushALL| clearLoopDetectAlarm>`** command.

Variable	Value
port	Specifies the port.
none	Specifies none.
flushMacFdb	Flushes MAC forwarding table for port.
flushALL	Flushes all tables.
clearLoopDetectAlarm	Clears loop detect alarm.

Command mode

Interface configuration mode

auto-negotiate

Use this command to enable autonegotiation (adjusting between 10 Mb/s and 100 Mb/s and half- or full-duplex) on selected ports.

Syntax

```
auto-negotiate [port <port list>]
```

Variable definitions

Use the following table to help you use the **`auto-negotiate [port <port list>]`** command.

Variable	Value
<port list>	specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*

Command mode

Interface configuration mode

no auto-negotiate

Use this command to disable autonegotiation on selected ports.

Syntax

```
no auto-negotiate [port <port list>]
```

Variable definitions

Use the following table to help you use the **no auto-negotiate [port <port list>]** command.

Variable	Value
<port list>	specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*

Command mode

Interface configuration mode

auto-recover-port

Use this command to enable auto recovery on ports.

Syntax

auto-recover-port [port *<portlist>***] [enable]**

Variable definitions

Use the following table to help you use the **auto-recover-port [port** *<portlist>***] [enable]** command.

Variable	Value
[port *<portlist>*]	specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*
[enable]	Enables auto recovery. The default is disabled.

Command mode

Interface configuration mode

default auto-recover-port

Use this command to set auto recovery on ports to default values.

Syntax

default auto-recover-port [port *<portlist>***] [enable]**

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **auto-recover-port [port** <*portlist*>**] [enable]** command.

Variable	Value
[port <*portlist*>]	specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*
[enable]	Enables auto recovery. The default is disabled.

Command mode

Interface configuration mode

no auto-recover-port

Use this command to remove auto recovery on ports.

Syntax

no auto-recover-port [port <*portlist*>**] [enable]**

Variable definitions

Use the following table to help you use the **no auto-recover-port [port** <*portlist*>**] [enable]** command.

Variable	Value
[port <*portlist*>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*
[enable]	Disables auto recovery. The default is disabled.

Command mode

Interface configuration mode

bcast-mcast-rate-limit

Use this command to enable broadcast and multicast rate limit on the ports.

Syntax

```
bcast-mcast-rate-limit <value> [port <port list>]
```

Variable definitions

Use the following table to help you use the **bcast-mcast-rate-limit <value> [port <port list>]** command.

Variable	Value
<*value*>	Value is the broadcast-rate-limit with a range of 1 to 100.
[port <*port list*>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Interface configuration mode

cp-limit

Use this command to enable Control Packet rate Limit (CP-Limit).

Syntax

cp-limit [port <*port list*> **]**

Variable definitions

Use the following table to help you use the **cp-limit [port** <*port list*> **]** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}

Command mode

Interface configuration mode

no cp-limit

Use this command to disable Control Packet rate Limit (CP-Limit).

Syntax

no cp-limit [port <*portlist*> **]**

Comments? infodev@avaya.com

Important:

After a CP-Limit is disabled on a port, it can only be re-enabled by disabling and re-enabling the port with command:

shutdown [port <ports>]

Variable definitions

Use the following table to help you use the **no cp-limit [port** *<port list>* **]** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}

Command mode

Interface configuration mode

default-vlan-id

Use this command to define the default Virtual LAN (VLAN) identification on selected ports.

Important:

The default switch configuration includes a port-based VLAN that includes all the ports in the system. This VLAN has a VID of 1 and is referred to as the Default VLAN. This VLAN is special in the sense that it cannot be deleted from the system, and that it is statically bound to the Default STG.

You should not confuse that Default VLAN with this default-vlan-id parameter. The purpose of this parameter is to place an incoming data packet into a user-defined (default) VLAN if the packet is expected to be carrying a VLAN ID and this value cannot be determined by the switch.

Syntax

default-vlan-id [port *<ports>* **]** *<vid>*

Variable definitions

Use the following table to help you use the **default-vlan-id [port** *<ports>* **]** *<vid>* command:

Variable	Value
[port *<ports>*]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
<vid>	Specifies the VLAN ID The range of values is 1 to 2000

Command mode

Interface configuration mode

duplex

Use this command to set the operating mode of the selected port to half-duplex or full-duplex when autonegotiation is disabled.

Syntax

duplex [port <*ports*> **] <half|full>**

Variable definitions

Use the following table to help you use the **duplex [port** <*ports*> **] <half|full>** command:

Variable	Value
[port <*ports*>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

half	Sets the operating mode of the specified port to half-duplex when autonegotiation is disabled. The default is half-duplex.
full	Sets the operating mode of the specified port to full-duplex when autonegotiation is disabled. The default is half-duplex.

Command mode

Interface configuration mode

eapol

Use this command to configure EAPoL on a specific port.

Syntax

eapol [guest-vlan<*vid*> **[port** <*portlist*> **] [init] [max-request <1....10>] [quiet-interval <1...65535] [re-authenticate] [re-authentication <enable|disable>] [re-authentication-period <1...2147483647>] [server-timeout <1...65535>] [supplicant-timeout <1...65535>] [traffic-control <in|in-out>] [transmit-interval <1...65535>]**

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **eapol [guest-vlan**<*vid*> **[port** <*portlist*> **] [init] [max-request <1....10>] [quiet-interval <1...65535] [re-authenticate] [re-authentication <enable|disable>] [re-authentication-period <1...2147483647>] [server-timeout <1...65535>] [supplicant-timeout <1...65535>] [traffic-control <in|in-out>] [transmit-interval <1...65535>]** command:

Variable	Value
guest-vlan <*vid*>	Specifies the ID of the guest VLAN.
init	Reinitializes EAPoL authentication on this port.
max-request <1...10>	Sets the maximum number of times to retry sending packets to the Supplicant. The default is 2.
port <portlist>	Enter the port or ports you want to configure for EAPoL, and use the convention {slot/port[-slot/port][,...]}. **Important:** If you omit this parameter, the system uses the port number specified when you entered the interface command.
quiet-interval <1...65535>	Sets the time interval (in seconds) between authentication failure and the start of a new authentication. The default is 60.
re-authenticate	Re-authenticates the Supplicant connected to this port immediately. **Important:** Before you can reauthenticate the Supplicant connected to this port, you must first enable reauthentication re-authentication <enable|disable>
re-authentication <*enable*|*disable*>	When enabled, re-authenticates an existing Supplicant at the time interval specified in re-authentication-period <1...2147483647> The default is disable.
re-authentication-period <*1...2147483647*>	Sets the time interval (in seconds) between successive re-authentications re-authentication <enable|disable>. The default is 3600 (1 hour).
server-timeout <1...65535>	Sets the time (in seconds) to wait for a response from the RADIUS server.

Variable	Value
	The default is 30.
status <auto|unauthorized|authorized>	Sets the authentication status for this port. The default is authorized. • auto - port authorization depends on the results of the EAPoL authentication by the RADIUS server. • unauthorized - port is always unauthorized. • authorized - port is always authorized.
supplicant-timeout <1...65535>	Sets the time (in seconds) to wait for a response from a Supplicant for all EAP packets except EAP Request/Identity packets. The default is 30.
traffic-control <in|in-out>	Sets the desired level of traffic control for a port. • in - Blocks incoming traffic when EAP authentication fails. • in-out- Blocks incoming and outgoing traffic when EAP authentication fails.
transmit-interval <1...65535>	Sets the time (in seconds) to wait for a response from a Supplicant for EAP Request/Identity packets. The default is 30.

Command mode

Interface configuration mode

no eapol

Use this command to disable eapol globally on the switch.

Syntax

`no eapol [port` <*port list*> **`]`**

Variable definitions

Use the following table to help you use the **`no eapol [port`** <*port list*> **`]`** command:

Comments? infodev@avaya.com

Variable	Value
[port <*port list*>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

encapsulation

Use this command to enable encapsulation on selected ports.

Syntax

`encapsulation [port` <*port list*> **`]`**

Variable definitions

Use the following table to help you use the **`encapsulation [port`** <*port list*> **`]`** command:

Variable	Value
[port <*port list*>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

no encapsulation

Use this command to disable encapsulation on selected ports.

Syntax

`no encapsulation [port` <*port list*> **`]`**

Variable definitions

Use the following table to help you use the **`no encapsulation [port`** <*port list*> **`]`** command:

Variable	Value
[port <*port list*>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

linktrap

Use this command to enable the link up/down trap of a specific port.

Syntax

`linktrap [port` *<port list>* **`]`**

Variable definitions

Use the following table to help you use the **`linktrap [port`** *<port list>* **`]`** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

no linktrap

Use this command to disable the link up/down trap of a specific port.

Syntax

`no linktrap [port` *<port list>* **`]`**

Variable definitions

Use the following table to help you use the **`no linktrap [port`** *<port list>* **`]`** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

Comments? infodev@avaya.com

lock

Use this command to lock the selected port or ports for exclusive use if the portlock feature is globally enabled.

Syntax

lock [port <*port list*> **]**

Variable definitions

Use the following table to help you use the **lock [port** <*port list*> **]** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

no lock

Use this command to unlock the selected port or ports from exclusive use if the portlock feature is globally enabled.

Syntax

no lock [port <*port list*> **]**

Variable definitions

Use the following table to help you use the **no lock [port** <*port list*> **]** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

name

Use this command to assign a name to the selected ports.

Syntax

`name [port` *<ports>* **`]`** *<name>*

Variable definitions

Use the following table to help you use the **`name [port`** *<ports>* **`]`** *<name>* command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.
<name>	Specifies the name of the port. The range of values is a string of 0 to 20 characters.

Command mode

Interface configuration mode

shutdown

Use this command to disable the interface on selected ports.

Syntax

`shutdown [port` *<ports>* **`]`**

Variable definitions

Use the following table to help you use the **`shutdown [port`** *<port list>* **`]`** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

Comments? infodev@avaya.com

no shutdown

Use this command to enable the interface on selected ports.

Syntax

no shutdown [port <*ports*> **]**

Variable definitions

Use the following table to help you use the **no shutdown [port** <*port list*> **]** command:

Variable	Value
[port <port list>]	specifies the applicable ports in port list form: {*slot/port [-slot/port][, ...]*}.

Command mode

Interface configuration mode

boot config flags spanning-tree-mode

Configures STP mode to set the spanning tree mode for the switch to Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or the default mode. The default mode is regular STP.

Syntax

boot config flags spanning-tree-mode

Variable definitions

Use the following table to help you use the **boot config flags spanning-tree-mode** command:

Variable	Value
mstp	Specifies MSTP, spanning tree mode.
rstp	Specifies RSTP, spanning tree mode.

Command mode

Global configuration mode

no boot config flags spanning-tree-mode

Disable STP mode to discontinue using spanning tree mode on the switch.

Syntax

no boot config flags spanning-tree-mode

Command mode

Global configuration mode

spanning-tree bpdu-filtering

Use this command to enable STP BPDU filtering.

Syntax

spanning-tree bpdu-filtering

Variable definitions

The following table defines optional parameters that you enter with the **spanning-tree bpdu-filtering** command.

Variable	Value
enable	Enables STP BPDU filtering on a port or group of ports.
port <portlist>	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Interface Configuration mode

no spanning-tree bpdu-filtering

Use this command to disable STP BPDU filtering.

Syntax

no spanning-tree bpdu-filtering

Comments? infodev@avaya.com

Variable definitions

The following table defines optional parameters that you enter with the **no spanning-tree bpdu-filtering** command.

Variable	Value
enable	Enables STP BPDU filtering on a port or group of ports.
port <portlist>	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Interface Configuration mode

spanning-tree bpdu-filtering timeout

Use this command to configure the STP BPDU filtering port timer.

Syntax

spanning-tree bpdu-filtering [timeout <10-65535|0>]

Variable definitions

The following table defines optional parameters that you enter with **spanning-tree bpdu-filtering [timeout <0-65535>]** command.

Variable	Value
<0-65535>	Specifies the STP BPDU Filtering port timer timeout duration in seconds. Values can be 0 or range from 0 to 65535. With timeout value of 0 configured, the STP BPDU Filtering port timer timeout duration is infinite.

Command mode

Interface Configuration mode

no spanning-tree bpdu-filtering timeout

Use this command to disable the STP BPDU filtering port timer.

Syntax

`no spanning-tree bpdu-filtering [timeout <10-65535|0>]`

Variable definitions

The following table defines optional parameters that you enter with **`no spanning-tree bpdu-filtering [timeout <0-65535>]`** command.

Variable	Value
<0-65535>	Specifies the STP BPDU Filtering port timer timeout duration in seconds. Values can be 0 or range from 0 to 65535. With timeout value of 0 configured, the STP BPDU Filtering port timer timeout duration is infinite.

Command mode

Interface Configuration mode

default spanning-tree bpdu-filtering

Use this command to configure the STP BPDU filtering default values.

Syntax

`default spanning-tree bpdu-filtering`

Variable definitions

The following table defines optional parameters that you enter with **`spanning-tree bpdu-filtering`** command.

Variable	Value
enable	Enables STP BPDU Filtering on a port or group of ports.
port <portlist>	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.
timeout <0-65535>	Specifies the STP BPDU Filtering port timer timeout duration in seconds. Values can be 0 or range from 0 to 65535. With timeout value of 0 configured, the STP BPDU Filtering port timer timeout duration is infinite.

Command mode

Interface Configuration mode

show spanning-tree bpdu-filtering

Use this command to display STP BPDU Filtering status information.

Syntax

`show spanning-tree bpdu-filtering [<interface-type>] [<portlist>]`

Variable definitions

The following table defines optional parameters that you enter with the **`show spanning-tree bpdu-filtering [<interface-type>] [<portlist>]`** command.

Variable	Value
<interface-type>	Identifies the type of interface for which to display port ARP inspection status. Values are FastEthernet and GigabitEthernet.
<portlist>	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Privileged EXEC mode

spanning-tree mstp

Configures the ports in a specified Spanning Tree Group (STG). This command can also display current settings for the port spanning tree group.

Syntax

`spanning-tree mstp`

Variable definitions

Use the following table to help you use the **`spanning-tree mstp`** command:

Variable	Value
forward-time <number>	Assigns the MSTP forward delay for the bridge from 400 to 3000 one hundredths of a second.

Variable	Value
max-age <number>	Assigns the MSTP maximum age time for the bridge from 600 to 4000 one hundredths of a second.
max-hop <number>	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second in steps of 100 one hundredths.
msti <number>	Assigns the MSTP MSTI instance parameter.
pathcost-type <16-bit|32-bit>	Assigns the MSTP default pathcost type to either 16 bits or 32 bits. The default is 32 bits.
priority <number>	Assigns the MSTP bridge priority in a range of 0 to 61440 in steps of 4096.
region <config-id-sel|regionname| region-version>	Assigns the MSTP region commands: • config-id-sel — Assigns the MSTP region configuration ID number: The range is 0 to 255. • region-name — Assigns the MSTP region name. The character string can be a range of 1 to 32 characters. • region-version — Assigns the MSTP region version. The range is 0 to 65535.
tx-holdcount <number>	Assigns the MSTP transmit hold count. The range is 1 to 10. The default is 3.
version <mstp|rstp|stp-compat ibler>	Assigns the MSTP bridge version.

Command mode

Global configuration mode

show spanning-tree mstp config

Use this command to view the MSTP configurations to display the MSTP-related bridge and region information.

Syntax

`show spanning-tree mstp config`

Comments? infodev@avaya.com

Command mode

Privileged EXEC mode

spanning-tree mstp cist

Configure Ethernet MSTP CIST to set the MSTP CIST parameters for a port.

Syntax

`spanning-tree mstp`

Variable definitions

Use the following table to help you use the **`spanning-tree mstp`** command:

Variable	Value
cost <intval>	Sets the CIST path cost parameter for the port in the range of 1 to 200000000.
edge-port<true|false>	Sets the MSTP edge-port parameter for the port.
force-port-state <enable>	Sets the state of the port to true (enabled) for the CIST .
hello-time <timeval>	Sets the hello time for a port from 100 to 1000 one hundredths of a second.
p2p <force-true|force-false|auto>	Sets the true or false Ethernet MSTP CIST point-to-point parameter for the port.
port	Specifies the port list.
priority	Assigns a priority for a port.
protocol-migration	Assigns the protocol migration as true or false for a port.

Command mode

Interface Configuration mode

no spanning-tree mstp cist

Disable Ethernet MSTP CIST to set the MSTP CIST parameters for a port.

Syntax

`no spanning-tree mstp force-port-state enable`

Command mode

Interface Configuration mode

spanning-tree mstp msti

Use this command to configure multi-service transport platform (MSTP) multiple spanning tree instance (MSTI) to set the configuration version.

Syntax

`spanning-tree mstp msti <instid>`

Variable definitions

Use the following table to help you use the **`spanning-tree mstp msti <instid>`** command:

Variable	Value
priority<*number*>	Assigns the MSTP bridge priority. The range is 0 to 65535, in steps of 4096.
<*instid*>	Specifies the MSTI instance ID.

Command mode

Global configuration mode

show spanning-tree mstp msti config

Use this command to view MSPT MSTI configuration information to review the MSTP instance status.

Syntax

`show spanning-tree mstp msti config <instid>`

Variable definitions

Use the following table to help you use the **`show spanning-tree mstp msti config <instid>`** command:

Variable	Value
<*instid*>	Specifies the MSTI instance ID.

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

spanning-tree mstp msti

Use this command to configure multi-service transport platform (MSTP) multiple spanning tree instance (MSTI) to set the configuration version.

Syntax

`spanning-tree mstp msti <instid>`

Variable definitions

Use the following table to help you use the **`spanning-tree mstp msti <instid>`** command:

Variable	Value
cost	Sets the MSTP MSTI path cost value for the port in the range of 1 to 200000000.
force-port-state enable	Enables MSTI learning for a port.
port <port>	Specifies a port or list of ports. Specify the port as: {slot/port[-slot/port][,...]}
priority<number>	Sets the Ethernet MSTP priority parameter for the port. The priority ranges in the range of 0 to 240 in steps of 16 (0, 16, 32, ... , 240).

Command mode

Interface configuration mode

show spanning-tree mstp port

Use this command to view the MSTP port role information to display the MSTP, CIST port roles and states information for a single port or a list of ports.

Syntax

`show spanning-tree mstp port <port>`

Variable definitions

Use the following table to help you use the **`show spanning-tree mstp port <port>`** command.

Variable	Value
config <portlist>	Displays MSTP CIST port information.
role <portlist>	Displays MSTP CIST port role and state information.
statistics	Displays MSTP port statistics.

Command mode

Privileged EXEC mode

show spanning-tree mstp status

Use this command to view the MSTP status to display bridge MSTP status information.

Syntax

`show spanning-tree mstp status`

Command mode

Privileged EXEC mode

spanning-tree rstp

Use this command to configure RSTP parameters to reduce recovery time after a network failure.

Syntax

`spanning-tree rstp`

Variable definitions

Use the following table to help you use the **`spanning-tree rstp`** command:

Variable	Value
forward-time <number>	Assigns the RSTP forward delay for the bridge from 400 to 3000 one hundredths of a second.
group-stp <enable>	Enables RSTP for a specific STG.
hello-time <number>	Assigns the RSTP hello time delay for the bridge from 100 to 1000 one hundredths of a second.

Variable	Value
max-age <number>	Assigns the RSTP maximum age time for the bridge from 600 to 4000 one hundredths of a second.
pathcost-type <16-bit|32-bit>	Assigns the RSTP default pathcost type to either 16 bits or 32 bits. The default is 32 bits.
priority <number>	Assigns the RSTP bridge priority in a range of 0 to 61440 in steps of 4096.
tx-holdcount	Assigns rstp tx holdcount.
version <rstp|stp-compatible>	Assigns the port in the RSTP- or STP-compatible mode; that is, whether the port transmits RSTP BPDUs or Config/TCN BPDUs.

Command mode

Global configuration mode

no spanning-tree rstp

Use this command to configure RSTP parameters to reduce recovery time after a network failure.

Syntax

`no spanning-tree rstp group-stp enable`

Command mode

Global configuration mode

show spanning-tree rstp config

Use this command to view global RSTP configuration to display RSTP configuration details for the switch.

Syntax

`show spanning-tree rstp config`

Command mode

Privileged EXEC mode

show spanning-tree rstp status

Use this command to view global RSTP status to display RSTP status information for the switch.

Syntax

`show spanning-tree rstp status`

Command mode

Privileged EXEC mode

spanning-tree rstp on port

Use this command to configure Ethernet RSTP parameters.

Syntax

`spanning-tree rstp`

Variable definitions

Use the following table to help you use the **`spanning-tree rstp`** command:

Variable	Value
cost <value>	Sets the RSTP path cost parameter for the port in the range of 1 to 200000000.
edge-port <true|false>	Sets the RSTP edge port parameter for the port.
p2p <force-true|force-false|auto>	Sets the Ethernet RSTP point-to-point parameter for the port.
<*slot/port*>	Defines the port on which to configure RSTP.
priority <value>	Sets the Ethernet RSTP priority parameter for the port. The priority ranges in the range of 0 to 240 in steps of 16 (0, 16, 32, ... , 240).
protocol-migration <true|false>	Sets the Ethernet RSTP protocol-migration parameter for the port.
stp <enable>	Enables STP on the port.

Command mode

Interface Configuration mode

no spanning-tree rstp on port

Use this command to configure Ethernet RSTP parameters.

Syntax

no spanning-tree rstp

Variable definitions

Use the following table to help you use the **no spanning-tree rstp** command:

Variable	Value
<*slot/port*>	Defines an Ethernet port on which to disable RSTP. Use the format: {slot/port}
stp	Disables STP on the port.

Command mode

Interface Configuration mode

show spanning-tree rstp port

Use this command to view port RSTP information to display RSTP parameter details for a specific port.

Syntax

show spanning-tree rstp port

Variable definitions

Use the following table to help you use the **show spanning-tree rstp port** command.

Variable	Value
config <portlist>	Displays the RSTP configuration for a port or list of ports. Specify the portlist as: {slot/port[-slot/p ort][,...]}
role <portlist>	Displays the RSTP role for a port or list of ports. Specify the portlist as: {slot/port[-slot/p ort][,...]}

Variable	Value
status <portlist	Displays the RSTP status for a port or list of ports. Specify the portlist as: {slot/port[-slot/p ort][,...]}

Command mode

Privileged EXEC mode

tx-queue

Use this command to configure transmit queue parameters for the specified ethernet port or ports.

Syntax

`tx-queue [port` *<ports>* **`] <queue-id>`**

Variable definitions

Use the following table to help you use the **`tx-queue [port`** *<ports>* **`] <queue-id>`** command:

Variable	Value
[port <ports>]	Specify the ports in the portlist form {*slot/port[-slot/port][, ...]*}.
queue-id	Specifies the queue ID, which represents a priority with a value range of 0 (lowest) to 7 (highest).

Command mode

Interface fastethernet mode

no tx-queue

Disables transmit queue parameters for the specified ethernet port or ports.

Syntax

`no tx-queue [port` *<ports>* **`]`** *<queue-id>*

Variable definitions

Use the following table to help you use the **`no tx-queue [port`** *<ports>* **`] <queue-id>`** command:

Comments? infodev@avaya.com

Variable	Value
[port <ports>]	Specify the ports in the portlist form {*slot/port[-slot/port][, ...]*}.
queue-id	Specifies the queue ID, which represents a priority with a value range of 0 (lowest) to 7 (highest).

Command mode

Interface configuration mode

unknown-mac-discard

Use this command to configure the unknown-mac-discard option on selected ports.

Syntax

unknown-mac-discard [port <*ports*> **] [activation] [add-allow-mac <0x00:0x00:0x00:0x00:0x00:0x00>][autolearn] [autolearn-mode <one-shot|continuous>] [lock-autolearn-mac] [violation-downport] [violation-logging] [violation-sendAuthentificationTrap]**

Variable definitions

Use the following table to help you use the **unknown-mac-discard [port** <*ports*> **] [activation] [add-allow-mac <0x00:0x00:0x00:0x00:0x00:0x00>] [autolearn] [autolearn-mode <one-shot|continuous>] [lock-autolearn-mac] [violation-downport] [violation-logging] [violation-sendAuthentificationTrap]** command:

Variable	Value
activation	Sets unknown MAC discard.
add-allow-mac <0x00:0x00:0x00:0x00:0x00:0x00>	Sets the add allow mac address of this port.
autolearn	Sets autolearn on this port.
autolearn-mode <one-shot|continuous>	Sets the autolearn mode.
lock-autolearn-mac <enable|disable>	Sets the lock autolearn MAC address of this port.
port <ports>	Specifies the port numbers which are to be changed
violation-downport	Sets violation down port action of this port.
violation-logging	Sets violation logging action of this port.

Variable	Value
violation-sendAuthentificationTrap	Sets violation send authentication action of this port.

Command mode

Interface configuration mode

no unknown-mac-discard

Use this command to disable the unknown-mac-discard option on selected ports.

Syntax

no unknown-mac-discard [port <*ports*> **] [activation] [autolearn] [autolearn-mode <one-shot|continuous>] [lock-autolearn-mac] [max-mac-count** <*max MAC count*> **] [remove-allow-mac** <*mac*> **] [violation-downport] [violation-logging] [violation-sendAuthentificationTrap]**

Variable definitions

Use the following table to help you use the **no unknown-mac-discard [port** <*ports*> **] [activation] [autolearn] [autolearn-mode <one-shot|continuous>] [lock-autolearn-mac] [max-mac-count** <*max MAC count*> **] [remove-allow-mac** <*mac*> **] [violation-downport] [violation-logging] [violation-sendAuthentificationTrap]** command:

Variable	Value
activation	Sets unknown MAC discard.
autolearn	Sets autolearn on this port.
autolearn-mode <one-shot|continuous>	Sets the autolearn mode.
lock-autolearn-mac <enable|disable>	Sets the lock autolearn MAC address of this port.
max-mac-count <*max MAC count*>	Sets the maximum number of MAC addresses allowed on this port.
remove-allow-mac <*mac*>	Removes allow MAC address from this port.
violation-downport	Sets violation down port action of this port.
violation-logging	Sets violation logging action of this port.
violation- sendAuthentificationTrap	Sets violation send authentication action of this port.

Comments? infodev@avaya.com

Command mode

Interface configuration mode

test loopback

Enables loopback test on specified ports.

Syntax

```
test loopback <ports>
```

ports

Variable definitions

Use the following table to help you use the **`test loopback <ports>`** command.

Variable	Value
ports	Specify the ports in the portlist form {slot/port[-slot/port][, ...]}.

Command mode

Interface configuration mode

test stop

Disables loopback test on specified ports.

Syntax

```
test stop <ports>
```

Variable definitions

Use the following table to help you use the **`test stop <ports>`** command.

Variable	Value
ports	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Interface configuration mode

untagged-frames-discard

Use this command to enable the discard untagged frames option on selected ports.

Syntax

`untagged-frames-discard [port` *<ports>* **`] <enable|disable>`**

Variable definitions

Use the following table to help you use the **`untagged-frames-discard [port`** *<ports>* **`] <enable|disable>`** command.

Variable	Value
[port <ports>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Interface configuration mode

no untagged-frames-discard

Use this command to disable the discard untagged frames option on selected ports.

Syntax

`no untagged-frames-discard [port` *<ports>* **`] <enable|disable>`**

Variable definitions

Use the following table to help you use the **`no untagged-frames-discard [port`** *<ports>* **`] <enable|disable>`** command.

Variable	Value
[port <ports>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Interface configuration mode

Comments? infodev@avaya.com

Chapter 8: Security commands

This chapter describes ACLI security commands and their parameters.

Navigation

- access-policy disable on page 167
- access-policy info on page 167
- access-policy policy on page 167
- access-policy policy create on page 169
- access-policy policy info on page 170
- eapol default-guest-vlan on page 171
- eapol guest-vlan on page 171
- eapol allow-non-eap mac-max on page 172
- eapol non-eap-mac add on page 172
- no eapol guest-vlan on page 172
- eapol guest-vlan-id on page 172
- eapol multihost on page 173
- eapol guest-vlan on page 173
- eapol multihost mac-max on page 173
- eapol allow-non-eap on page 173
- no access-policy policy on page 177
- no eapol allow-non-eap on page 177
- no eapol guest-vlan on page 177
- no eapol multihost on page 178
- no eapol non-eap-mac on page 178
- no nsna on page 180
- no nsna enable on page 180
- no nsna nsnas on page 180
- no nsna phone-signature on page 181

- no nsna vlan on page 181
- no radius on page 182
- no radius-server on page 182
- no snmp-server v1v2 community on page 182
- no syslog host on page 183
- nsna on page 183
- nsna enable on page 184
- nsna nsnas on page 184
- nsna phone-signature on page 185
- nsna uplink vlans on page 185
- nsna vlan color on page 186
- nsna fail-open vlan-id on page 186
- nsna fail-open enable on page 187
- no nsna fail-open on page 187
- radius on page 187
- radius clear-stat on page 188
- radius info on page 189
- radius-server info on page 189
- snmp-server group info on page 189
- snmp-server group match on page 189
- snmp-server group view on page 190
- snmp-server info on page 191
- snmp-server member info on page 191
- snmp-server member name on page 192
- snmp-server user auth on page 192
- snmp-server user info on page 193
- snmp-server user priv on page 193
- snmp-server view info on page 194
- snmp-server view mask on page 194
- snmp-server view type on page 195
- syslog host on page 196
- syslog host create on page 196
- syslog host severity on page 197

access-policy disable

Use this command to globally disable the IP access policy feature on the switch so that no policies on the switch are applied. The default is disabled.

Syntax

```
access-policy disable
```

Command mode

Global configuration mode

access-policy enable

Use this command to globally enable the IP access policy feature on the switch. The default is disabled.

Syntax

```
access-policy enable
```

Command mode

Global configuration mode

access-policy info

Use this command to display the global access policy settings.

Syntax

```
access-policy info
```

Command mode

Global configuration mode

access-policy policy

Use this command to specify access level policies for different methods of access.

Syntax

access-policy policy <*vid*> **[ftp <enable|disable>] [http <enable|disable>] [rlogin <enable|disable>] [snmp <enable|disable>] [telnet <enable|disable>] [tftp <enable|disable>]**

Variable definitions

Use the following table to help you use the **access-policy policy** <*vid*> **[ftp <enable|disable>] [http <enable|disable>] [rlogin <enable|disable>] [snmp <enable|disable>] [telnet <enable|disable>] [tftp <enable|disable>]** command.

Variable	Value
<*vid*>	Specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535
[ftp <enable|disable>]	Enables or disables access to ftp network communication protocols for the specified policy.
[http <enable|disable>]	Enables or disables access to http network communication protocols for the specified policy.
[rlogin <enable|disable>]	Enables or disables access to rlogin network communication protocols for the specified policy.
[snmp-group WORD <1-32>]	Adds an SNMP-V3 group under the specific access policy. WORD <1-32> is the name the SNMP-V3 group.
[snmpv3 <enable|disable>]	Enables or disables SNMP-V3.
[ssh <enable|disable>]	Enables or disables SSH.
[telnet <enable|disable>]	Enables or disables access to telnet network communication protocols for the specified policy.
[tftp <enable|disable>]	Enables or disables access to tftp network communication protocols for the specified policy.

Command mode

Global configuration mode

Comments? infodev@avaya.com

access-policy policy create

Use this command to create an IP access policy with a specified access policy ID. This command sets accesslevel policies.

Syntax

access-policy policy <*vid*> **create [name** <*name*> **] [<enable|disable>] [mode <allow|deny>] [precedence** <*value*> **] [network** <*ip/mask*> **] [host** <*ip*> **] [username** <*name*> **] [accesslevel** <*string*> **]**

Variable definitions

The following table describes variables that you enter in the **access-policy policy** <*vid*> **create [name** <*name*> **] [<enable|disable>] [mode <allow|deny>] [precedence** <*value*> **][network** <*ip/mask*> **][host** <*ip*> **] [username** <*name*> **] [accesslevel** <*string*> **]** command.

Variable	Value
<*vid*>	Specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535
[name <*name*>]	Specifies a name for the access policy. The range of values is a string of 0 to 15 characters.
[<enable|disable>]	Enables or disables the specified access policy.
[mode <allow|deny>]	Specifies the access policy mode. The options are: allow or deny.
[precedence <*value*>]	Specifies the access policy precedence. Precedence determines which policy to use if multiple policies apply. <*value*> specifies the precedence level. The range of values is 1 to 128, with the lowest number having the highest precedence.
[network <*ip/mask*>]	Specifies stations affected by the access policy using the network IP address and subnet mask. *ip* specifies the IP address {a.b.c.d} of the host used to authenticate the user. The login must be the specified user at the specified host for access. If you specify an IP address and subnet mask, that location is either allowed or

Variable	Value
	denied access, depending on the *mode* setting. The options are: {a.b.c.d/x| a.b.c.d/x.x.x.x| default}. *default* specifies that everyone on the network is either allowed or denied access, as defined by the mode setting.
[host <*ip*>]	Specifies the access policy for the trusted host address. Applies only for remote login and remote shell execution.
[username <*name*>]	Specifies the trusted host user name for the trusted host with the specified policy. Applies only to rlogin access
[accesslevel <*string*>]	Specifies an access level for a policy. The options are: {ro | rw | rwa} or {read-only| read-write | read-write-all}.

Command mode

Global configuration mode

access-policy policy info

Use this command to create an IP access policy with a specified access policy ID. Sets accesslevel policies.

Syntax

`access-policy policy` <*vid*> **`info`**

Variable definitions

The following table describes variables that you enter in the **`access-policy policy`** <*vid*> **`info`** command.

Variable	Value
<*vid*>	Specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535.

Command mode

Global configuration mode

Comments? infodev@avaya.com

default ip dhcp-snooping

Use this command to disable DHCP snooping on the switch.

Syntax

`default ip dhcp-snooping enable`

Command mode

Global Configuration mode

eapol default-guest-vlan

This command enables the EAPOL default guest VLAN.

Syntax

`eapol default-guest-vlan <vid>`

Variable definitions

Use the following table to help you use the **`eapol default-guest-vlan <vid>`** command

Variable	Value
<*vid*>	Specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535.

Command mode

Global configuration mode.

eapol guest-vlan

This command enables the EAPOL guest VLAN.

Syntax

`eapol guest-vlan`

Command mode

Global configuration mode.

eapol allow-non-eap mac-max

This command sets the maximum number of non-EAP clients.

Syntax

```
eapol allow-non-eap mac-max {<1-8>}
```

Command mode

Global configuration mode.

eapol non-eap-mac add

This command adds a non-EAP MAC Address to the allow list.

Syntax

```
eapol non-eap-mac add {<mac-add>}
```

no eapol guest-vlan

This command disables guest-vlan.

Syntax

```
no eapol guest-vlan
```

Command mode

This command is in the Interface configuration mode.

eapol guest-vlan-id

This command sets the guest-vlan at port level

Syntax

n

Command mode

This command is in the Interface configuration mode.

eapol multihost

This command enables EAPOL multihost.

Syntax

```
eapol multihost
```

eapol guest-vlan

This command enables guest-vlan

Syntax

```
eapol guest-vlan
```

Command mode

This command is in the Interface Config mode.

eapol multihost mac-max

This command sets the maximum number of EAP clients. The default is 1.

Syntax

```
eapol multihost mac-max {<1-8>}
```

eapol allow-non-eap

This command allows non-EAP clients.

Syntax

```
eapol allow-non-eap
```

ip arp-inspection vlan

Use this command to enable dynamic ARP inspection on a VLAN.

Syntax

ip arp-inspection vlan <vid>

Variable definitions

The following table defines parameters that you enter with the **ip arp-inspection vlan <vid>** command.

Variable	Value
<vid>	An integer that identifies a VLAN. Values range from 1 to 4000.

Command mode

Global Configuration mode

ip arp-inspection

Use this command to configure port ARP status.

Syntax

ip arp-inspection [port <portlist>] <trusted|untrusted>

Variable definitions

The following table defines parameters that you enter with the **ip arp-inspection [port <portlist>] <trusted|untrusted>** command.

Variable	Value
<portlist>	Specifies a single port or range of ports, entered as {slot/port[-slot/ port][,...]}.
<trusted>	Specifies that ARP traffic is not subject to dynamic ARP inspection.
<untrusted>	Specifies that ARP traffic is subject to dynamic ARP inspection.

Command mode

Interface Configuration mode

ip dhcp-snooping (global)

Use this command to enable DHCP snooping globally.

Syntax

`ip dhcp-snooping`

OR

`ip dhcp-snooping enable`

Command mode

Global Configuration mode

ip dhcp-snooping (interface)

Use this command to configure port-based DHCP snooping.

Syntax

`ip dhcp-snooping`

Variable definitions

The following table defines optional parameters that you enter with the **`ip dhcp-snooping`** command.

Variable	Value
[port <portlist>]	Specifies a single port or range of ports, entered as {slot/port[-slot/ port][,...]}.
<trusted>	Specifies that the DHCP snooping state for a port or ports is configured as trusted.
<untrusted>	Specifies that the DHCP snooping state for a port or ports is configured as untrusted.

Command mode

Interface Configuration mode

ip dhcp-snooping vlan

Use this command to enable VLAN-based DHCP snooping.

Syntax

`ip dhcp-snooping vlan <vid>`

OR

`ip dhcp-snooping vlan <vid> enable`

Variable definitions

The following table defines parameters that you enter with the **`ip dhcp-snooping vlan <vid>`** and **`ip dhcp-snooping vlan <vid> enable`** commands.

Variable	Value
<*vid*>	An integer that identifies a VLAN. Values range from 1 to 4000.

Command mode

Global Configuration mode

ip verify source interface

Use this command to enable IP Source Guard.

Syntax

`ip verify source interface [{<interface type>} {<portlist>}]`

Variable definitions

The following table defines parameters that you enter with the **`ip verify source [interface {<interface type>} {<portlist>}]`** command.

Variable	Value
<interface type>	Identifies the interface on which you want IP Source Guard enabled. Values are FastEthernet and GigabitEthernet.
<portlist>	Specifies a single port or range of ports, entered as {slot/port[-slot/ port][,...]}.

Comments? infodev@avaya.com

Command mode

Interface Configuration mode

no access-policy policy

Use this command to delete access policies for a specific policy ID.

Syntax

`no access-policy policy` <*pid*>

Variable definitions

Use the following table to help you use the **`no access-policy policy`** <*pid*> command.

Variable	Value
<*pid*>	specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535.

Command mode

Global configuration mode

For more information about access policies, see *Configuring and Managing Security using the ACLI and CLI (316804-C)*.

no eapol allow-non-eap

This command disallows non-EAP clients.

Syntax

`no eapol allow-non-eap`

no eapol guest-vlan

This command disables the EAPOL guest VLAN.

Syntax

`no eapol guest-vlan`

Command mode

This command is in the Global Config mode.

no eapol multihost

This command disables EAPOL multihost.

Syntax

```
no eapol multihost
```

no eapol non-eap-mac

This command removes a non-EAP MAC Address from the allow list.

Syntax

```
np eapol non-eap-mac {<mac-add>}
```

no ip arp-inspection vlan

Use this command to disable dynamic ARP inspection on a VLAN.

Syntax

`no ip arp-inspection vlan`

Variable definitions

The following table defines parameters that you enter with the **`no ip arp-inspection vlan`** command.

Variable	Value
<cr>	Disables dynamic ARP inspection on all VLANs configured on the switch.
<*vid*>	An integer that identifies a specific VLAN. Values range from 1 to 4000.

Command mode

Global Configuration mode

Comments? infodev@avaya.com

no ip dhcp-snooping

Use this command to disable DHCP snooping on the switch.

Syntax

no ip dhcp-snooping

Command mode

Global Configuration mode

no ip dhcp-snooping vlan

Use this command to disable VLAN-based DHCP snooping.

Syntax

no ip dhcp-snooping vlan <vid>

Variable definitions

The following table defines parameters that you enter with the **no ip dhcp-snooping vlan <vid>** command.

Variable	Value
<*vid*>	An integer that identifies a VLAN. Values range from 1 to 4000.

Command mode

Global Configuration mode

no ip verify source interface

Use this command to disable IP Source Guard.

Syntax

no ip verify source interface [{<interface type>} {<portlist>}]

Variable definitions

The following table defines optional parameters that you enter after the **no ip verify source interface [{<interface type>} {<portlist>}]** command.

Variable	Value
`<interface type>`	Identifies the interface on which you want IP Source Guard disabled.
`<portlist>`	Identifies the ID of the interface on which you want IP Source Guard disabled.

Command mode

Interface Configuration mode

no nsna

Use this command to remove an NSNA port.

Syntax

```
no nsna
```

Command mode

Ethernet Interface configuration mode

no nsna enable

Use this command to disable NSNA.

Syntax

```
no nsna enable
```

Command mode

Global configuration mode

no nsna nsnas

Use this command to remove the NSNAS 4050 subnet.

Syntax

```
no nsna nsnas <ipaddr/mask>
```

Variable definitions

Use the following table to help you use the **`no nsna nsnas <ipaddr/mask>`**command

Comments? infodev@avaya.com

Variable	Value
<ipaddr/mask>	Specifies the NSNAS 4050 IP address and network mask (a.b.c.d/<0-32>).

Command mode

Global configuration mode

no nsna phone-signature

Use this command to remove NSNA phone signatures.

Syntax

```
no nsna phone-signature <LINE>
```

Variable definitions

Use the following table to help you use the **no nsna nsnas <ipaddr/mask>**command

Variable	Value
<LINE>	Specifies the is the phone signature string (for example: Avaya-i2007-A).

no nsna vlan

Use this command to remove an NSNA VLAN.

Syntax

```
no nsna vlan <vid>
```

Variable definitions

Use the following table to help you use the **no nsna vlan <vid>** command

Variable	Value
<vid>	Specifies the VLAN ID in the range 1-4000.

Command mode

Global configuration mode

no radius

Use this command to remove CLI commands from accounting requests for Remote Access Dial-in User Services (RADIUS).

Syntax

```
no radius acct-include-cli-commands
```

Command mode

Global configuration mode

no radius-server

Use this command to disable the IP address for Remote Access Dial-in User Services (RADIUS) on the server.

Syntax

`no radius-server` <*ipaddr*>

Variable definitions

Use the following table to help you use the **`no radius-server`** <*ipaddr*> command.

Variable	Value
`<ipaddr>`	Specifies the IP address for RADIUS on the server.

Command mode

Global configuration mode

For more information about RADIUS operations, see *Configuring and Managing Security using the ACLI and CLI (316804-C)*.

no snmp-server v1v2 community

Use this command to set the switch to check the v1v2 community string against the login access level.

Syntax

```
no snmp-server v1v2 community
```


Comments? infodev@avaya.com

Command mode

Global configuration mode

no syslog host

Use this command to delete a syslog host.

Syntax

`no syslog host` <*id*>

Variable definitions

Use the following table to help you use the **`no syslog host`** <*id*> command.

Variable	Value
<*id*>	Specifies the syslog host ID. The range of values is 1 to 10.

Command mode

Global configuration mode

nsna

Use this command to configure NSNA on ports.

Syntax

`nsna`

Variable definitions

Use the following table to help you use the **`nsna`** command.

Variable	Value
disable	Enables/disables the Avaya SNA state of the port.
dynamic [voip-vlans <value>]	Sets the Avaya SNAS 4050 dynamic port configuration, where <value> is the VoIP VLAN IDs (vlan-id[-vlan-id][,...]).
info	Shows the current Avaya SNA settings for the port.

Variable	Value
uplink uplink-vlans	Defines the Avaya SNAS 4050 uplink VLAN list, where <value> is the Avaya SNA VLAN IDs (vlan-id[-vlan-id][,...]).

Command mode

Interface fastethernet or gigabitethernet mode

nsna enable

Use this command to enable NSNA.

Syntax

```
nsna enable
```

Important:

You must enable SSH before you enable Avaya SNA globally. The command to enable Avaya SNA fails if you do not enable SSH.

Command mode

Global configuration mode

nsna nsnas

Use this command to configure the Avaya SNA 4050 subnet.

Syntax

```
nsna nsnas <ipaddr/mask>
```

Variable definitions

Use the following table to help you use the **`nsna nsnas <ipaddr/mask> port <value>`** command.

Variable	Value
<ipaddr/mask>	Specifies the Avaya SNAS 4050 pVIP address and network mask (a.b.c.d/<0-32> | a.b.c.d/x.x.x.x | default).

port <value>	Defines the TCP port number for the Switch to Avaya SNAS 4050 Communication

Comments? infodev@avaya.com

	Protocol (SSCP) server. Values are in the range 1024–65535. The default setting is 5000.

Command mode

Global configuration mode

nsna phone-signature

Use this command to specify IP phone signatures for the NSNA solution.

Syntax

```
nsna phone-signature <LINE>
```

Variable definitions

Use the following table to help you use the **`nsna phone-signature <LINE>`** command.

Variable	Value
<LINE>	Specifies the phone signature string (for example: Avaya-i2007-A).

Command mode

Global configuration mode

nsna uplink vlans

Use this command to add the uplink port to the NSNA VLANs. You must have the uplink filter configured before you add the uplink port to the VLANs.

Syntax

```
nsna uplink vlans <vidlist>
```

Variable definitions

Use the following table to help you use the **`nsna uplink vlans <vidlist>`** command.

Variable	Value
<vidlist>	Specifies the NSNA uplink VLAN IDs, entered using the convention {vlan-id[-vlan-id][,...]}.

Command mode

Interface fastethernet or gigabitethernet mode

nsna vlan color

Use this command to configure the NSNA VLANs.

Syntax

```
nsna vlan <vid> color <red|yellow|green|voip>
```

Variable definitions

Use the following table to help you use the **`nsna vlan <vid> color <red|yellow|green|voip>`** command.

Variable	Value
<vid>	Sets the VLAN ID in the range 2–4000.
<red|yellow|green|voip>	Specifies the color of the VLAN.

Command mode

Global configuration mode

nsna fail-open vlan-id

Use this command to configure the Fail Open VLAN ID.

syntax

`nsna fail-open vlan-id <1-4000> [filter-vlan-id <1-4000>`

Variable definitions

Use the data in the following table to help you use **`nsna fail-open vlan-id`** command.

Variable	Value
enable	Specifies the Fail Open state as enabled.
filter-vlan-id <1-4000>	Specifies the Fail Open VLAN ID.
vlan-id <1-4000>	Specifies the VLAN ID.

Command mode

Global configuration mode

nsna fail-open enable

Use this command to enable Fail Open.

syntax

nsna fail-open enable

Command mode

Global configuration mode

no nsna fail-open

Use this command to disable FAIL OPEN.

syntax

no nsna fail-open

Command mode

Global configuration mode

radius

Use this command to configure Remote Access Dial-in User Services (RADIUS) on the switch. This command can also display global RADIUS settings.

Syntax

radius [<enable|disable>] [attribute-value <*value*> **] [maxserver** <*INT*> **] [acct-enable|acct-disable] [acct-attribute-value** <*value*> **]**

Variable definitions

Use the following table to help you use the **radius [<enable|disable>] [attribute-value** <*value*> **] [maxserver** <*INT*> **] [acct-enable|acct-disable] [acct-attribute-value** <*value*> **]** command.

Variable	Value
[<enable|disable>]	Enables or disables the RADIUS authentication feature.

Variable	Value
[attribute-value <*value*>]	Specific to RADIUS authentication. Specifies the vendor-specific attribute value of the Access-Priority attribute to match the type value set in the dictionary file on the RADIUS server. Avaya recommends the default setting of 192 for Ethernet Routing Switch 8300Series switches. The range of values is 192 to 240.
[maxserver <*INT*>]	Specific to RADIUS authentication. Specifies the maximum number of servers allowed for the switch. The range of values is 1 to 10.
[acct-enable| acct-disable]	Enables or disables RADIUS accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. The default is acct-disable.
[acct-attribute-value <*value*>]	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. <*value*> must be different from the access-priority attribute value configured for authentication. The range of values is 192 to 240. The default value is 193.

Command mode

Global configuration mode

radius clear-stat

Use this command to clear statistics from the server for the Remote Access Dial-in User Services (RADIUS) on the switch.

Syntax

```
radius clear-stat
```

Command mode

Global configuration mode

Comments? infodev@avaya.com

radius info

Use this command to display global settings for the Remote Access Dial-in User Services (RADIUS) on the switch.

Syntax

```
radius info
```

Command mode

Global configuration mode

radius-server info

Use this command to display a list of all servers configured for Remote Access Dial-in User Services (RADIUS) on the switch.

Syntax

```
radius-server info
```

Command mode

Global configuration mode

snmp-server group info

Use this command to display current level parameter settings and next level directories for a Signaling Network Management Protocol (SNMP) group.

Syntax

```
snmp-server group info
```

Command mode

Global configuration mode

snmp-server group match

Use this command to change the group access context match in the v3 VACM table for a Signaling Network Management Protocol (SNMP) group.

Syntax

snmp-server group match <*group name*> <*prefix*> <*model*> <*level*> **[match** <*value*> **]**

Variable definitions

Use the following table to use the **snmp-server group match** <*group name*> <*prefix*> <*model*> <*level*> **[match** <*value*> **]** command.

Variable	Value
<*group name*>	Creates the new group access with this group name. The range of values is 1 to 32 characters.
<*prefix*>	Assigns a context prefix. The range of values is 1 to 32 characters.
<*model*>	Assigns the authentication checking to communicate to the switch. The options are: usm, snmpv1, and snmpv2c.
<*level*>	Assigns the minimum level of security required to gain access rights allowed by this conceptual row.
[match <*value*>]	Specifies the context match. The options are exact and prefix. • exact specifies that all rows in which the context name exactly matches the context prefix are selected. • prefix specifies that all rows in which the starting octet of the context name exactly matches the context prefix are selected.

Command mode

Global configuration mode

snmp-server group view

Use this command to change the group access view name match in the v3 VACM table for a Signaling Network Management Protocol (SNMP) group.

Syntax

snmp-server group view <*group name*> <*prefix*> <*model*> <*level*> **[read** <*value*> **]** **[write** <*value*> **]**

Comments? infodev@avaya.com

Variable definitions

Use the following to use the **`snmp-server group view`** <*group name*> <*prefix*> <*model*> <*level*> **`[read`** <*value*> **`] [write`** <*value*> **`]`** command.

Variable	Value
<*group name*>	Creates the new group access with this group name. The range of values is 1 to 32 characters.
<*prefix*>	Assigns a context prefix. The range of values is 1 to 32 characters.
<*model*>	Assigns the authentication checking to communicate to the switch. The options are: usm, snmpv1, and snmpv2c.
<*level*>	Specifies the minimum level of security required to gain access rights allowed by this conceptual row.
[read <*value*>]	
[write <*value*>]	

Command mode

Global configuration mode

snmp-server info

Use this command to display the current Signaling Network Management Protocol (SNMP) parameter settings.

Syntax

`snmp-server info`

Command mode

Global configuration mode

snmp-server member info

Use this command to display current level parameter settings and next level directories for Signaling Network Management Protocol (SNMP) group members.

Syntax

```
snmp-server member info
```

Command mode

Global configuration mode

snmp-server member name

Use this command to change a Signaling Network Management Protocol (SNMP) group member name for the v3 VACM table.

Syntax

snmp-server member name <*user name*> <*model*> <*group name*>

Variable definitions

Use the following to use the **snmp-server member name** <*user name*> <*model*> <*group name*>command

Variable	Value
<*user name*>	Assigns a user name to the SNMP member. The range of values is 1 to 32 characters.
<*model*>	Specifies the message processing model to use when generating an SNMP message. The options are: usm, snmpv1, and snmpv2c.
<*group name*>	Assigns the SNMP member to a SNMP group for data access. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

snmp-server user auth

Use this command to change the authentication password for a Signaling Network Management Protocol (SNMP) user on the switch.

Syntax

snmp-server user auth <*user name*> **old-pass** <*value*> **new-pass** <*value*>

Comments? infodev@avaya.com

Variable definitions

Use the following to use the **snmp-server user auth** <*user name*> **old-pass** <*value*> **new-pass** <*value*> command

Variable	Value
<*user name*>	Specifies the security name of the user whose authentication password is being changed. The security name is an index to the table. The range is 1 to 32 characters.
new-pass <*value*>	Specifies the new password.
old-pass <*value*>	Specifies the old password.

Command mode

Global configuration mode

snmp-server user info

Use this command to display current level parameter settings and next level directories for a Signaling Network Management Protocol (SNMP) user.

Syntax

```
snmp-server user info
```

Command mode

Global configuration mode

snmp-server user priv

Use this command to change the privacy password for a Signaling Network Management Protocol (SNMP) user on the switch.

Syntax

snmp-server user priv <*user name*> **old-pass** <*value*> **new-pass** <*value*>

Variable definitions

Use the following to use the **snmp-server user priv** <*user name*> **old-pass** <*value*> **new-pass** <*value*> command.

Variable	Value
<*user name*>	Specifies the security name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.
new-pass <*value*>	Specifies the new password.
old-pass <*value*>	Specifies the old password.

Command mode

Global configuration mode

snmp-server view info

Use this command to display the current level parameter settings and next level directories for the Management Information Base (MIB) view of the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

```
snmp-server view info
```

Command mode

Global configuration mode

snmp-server view mask

Use this command to change the view mask for an entry in the Management Information Base (MIB) View table for the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

`snmp-server view mask` <*view name*> <*subtree oid*> <*new-mask*>

Variable definitions

Use the following to use the **`snmp-server view mask`** <*view name*> <*subtree oid*> <*new-mask*> command.

Variable	Value
<*view name*>	Specifies the group name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.

Comments? infodev@avaya.com

Variable	Value
<*subtree oid*>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.
<*new-mask*>	Specifies the new bit mask used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.

Command mode

Global configuration mode

snmp-server view type

Use this command to change the type for an entry in the Management Information Base (MIB) View table for the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

`snmp-server view type` <*view name*> <*subtree oid*> <*new-type*>

Variable definitions

This command includes the following options:

Variable	Value
<*view name*>	Specifies the group name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.
<*subtree oid*>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.
<*new-type*>	Specifies the new view type used.

Command mode

Global configuration mode

syslog host

Use this command to configure a host location for the system log information (syslog) host.

Syntax

syslog host <*id*> **[address** <*ipaddr*> **] [udp-port** <*port*> **] [facility** <*facility*> **] [<enable|disable>]**

Variable definitions

Use the following to use the command

Variable	Value
<*id*>	Specifies the syslog host ID. The range of values is 1 to 10.
[address <*ipaddr*>]	Specifies the IP address of the UNIX system syslog host.
[udp-port <*port*>]	Specifies the UNIX system syslog host port number on which to send syslog messages to the syslog host. The range of values is 514 to 530.
[facility <*facility*>]	Specifies the UNIX system syslog host facility. The range of values is **LOCAL0** to **LOCAL7**.
[<enable|disable>]	Enables or disables sending syslog messages on the switch.

Command mode

Global configuration mode

syslog host create

Use this command to create a system log information (syslog) host and configure a host location.

Syntax

syslog host <*id*> **create [<enable|disable>] [address** <*ipaddr*> **] [facility** <*facility*> **] [udp-port** <*port*> **]**

Comments? infodev@avaya.com

Variable definitions

Use the following to use the command

Variable	Value
<*id*>	Specifies the syslog host ID. The range of values is 1 to 10.
[<enable|disable>]	Enables or disables the syslog host.
[address <*ipaddr*>]	Specifies the IP address of the UNIX system syslog host.
[facility <*facility*>]	Specifies the UNIX system syslog host facility. The range of values is LOCAL0 to LOCAL7.
[udp-port <*port*>]	Specifies the UNIX system syslog host port number on which to send syslog messages to the syslog host. The range of values is 514 to 530.

Command mode

Global configuration mode

syslog host severity

Use this command to specify the severity level of system log information (syslog) messages sent for the specified modules.

Syntax

`syslog host` <*id*> **`severity <info|warning|error|fatal> [<info|warning|error|fatal>] [<info|warning|error|fatal>] [<info|warning|error|fatal>]`**

Variable definitions

Use the following to use the command

Variable	Value
<*id*>	Specifies the syslog host ID. The range of values is 1 to 10.
<info|warning| error|fatal>	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.

Variable	Value
[<info|warning| error|fatal>]	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.
[<info|warning| error|fatal>]	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.
<info|warning| error|fatal>]	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 9: IP protocol commands

This chapter describes ACLI IP protocol commands and their Variable definitions.

Navigation

- accept adv-rtr on page 202
- area on page 203
- as-boundary-router enable on page 204
- default as-boundary-router enable on page 204
- no as-boundary-router enable on page 204
- auto-vlink enable on page 205
- default-metric on page 205
- default timer basic on page 206
- default default-metric on page 206
- host-route on page 207
- interface loopback on page 207
- ip address on page 208
- no ip address on page 208
- ip alternative-route on page 209
- no ip alternative-route on page 209
- ip arp on page 209
- no ip arp on page 210
- ip arp proxy on page 211
- no ip arp proxy on page 211
- ip arp response on page 211
- no ip arp response on page 211
- ip default-ttl on page 212
- ip dhcp-relay broadcast on page 212
- ip dhcp-relay on page 213

- ip dhcp-relay max-hop on page 213
- ip dhcp-relay min-sec on page 214
- ip dhcp-relay mode on page 214
- ip dhcp-relay fwd-path on page 214
- ip forward-protocol udp on page 218
- no ip forward-protocol udp on page 219
- ip forward-protocol udp portfwdlist on page 219
- no ip forward-protocol udp portfwdlist on page 220
- ip forward-protocol udp on page 221
- no ip forward-protocol udp on page 222
- ip forward-protocol udp portfwdlist on page 219
- ip icmp-unreach-msg on page 223
- no ip icmp-unreach-msg on page 223
- ip irdp enable on page 223
- no ip irdp enable on page 223
- ip irdp on page 224
- no ip irdp on page 224
- default ip irdp on page 225
- no ip irdp multicast on page 225
- ip irdp vlan multicast on page 225
- no ip irdp vlan multicast on page 226
- ip more-specific-non-local-route enable on page 226
- no ip more-specific-non-local-route enable on page 226
- ip ospf on page 227
- ip ospf spf-run on page 228
- ip prefix-list on page 229
- no ip prefix-list on page 230
- ip routing on page 230
- no ip routing on page 230
- ip rip on page 230
- ip route on page 234
- no ip route on page 235
- ip route preference protocol on page 235
- net6-mgmt ipv6 on page 236

- no net6-mgmt ipv6 on page 237
- no net6-mgmt ipv6 route on page 237
- net6-mgmt ipv6 route on page 238
- ipv6 mgmt-virtual on page 238
- lldp on page 239
- default lldp on page 239
- lldp port status on page 240
- no lldp status on page 241
- default lldp port on page 241
- lldp tx-tlv on page 242
- no lldp tx-tlv on page 242
- default lldp tx-tlv on page 243
- lldp tx-tlv dot1 on page 243
- no lldp tx-tlv dot1 on page 244
- default lldp tx-tlv dot1 on page 244
- lldp tx-tlv dot3 on page 244
- no lldp tx-tlv dot3 on page 245
- default lldp tx-tlv dot3 on page 245
- lldp tx-tlv med on page 246
- no lldp tx-tlv med on page 246
- default lldp tx-tlv med on page 247
- lldp location-identification civic-address on page 247
- manualtrigger ip rip interface vlan on page 248
- network on page 249
- no network on page 249
- network area on page 250
- redistribute enable on page 250
- redistribute source on page 251
- route-map on page 251
- no route-map on page 253
- router ospf on page 254
- router ospf enable on page 254
- no router ospf enable on page 254
- router rip on page 255

- router rip enable on page 255
- no router rip enable on page 255
- router-id on page 256
- slpp on page 256
- Default slpp on page 257
- no slpp on page 257
- slpp port on page 258
- default slpp port on page 258
- no slpp port on page 259
- timer basic on page 261
- timers basic holddown on page 262
- trap enable on page 263
- vlan nlb-mode on page 263
- no vlan nlb-mode on page 264

accept adv-rtr

Use this command to configures OSPF acceptance.

Syntax

```
accept adv-rtr <ipaddr>
```

Variable definitions

Use the following table to help you use the command.

Variable	Value
accept adv-rtr	Accept ospf router.
<ipaddr> enable	Enable OSPF accept on particular router. <ipaddr> is router ID.
<ipaddr> metric-type [type1|type2|any]	Set OSPF accept on particular router with particular metric type. <ipaddr> is router ID. [type1|type2|any] is metric type.
<ipaddr> route-policy WORD<0-64>	Set OSPF accept on particular router with particular routing policy. <ipaddr> is router ID. WORD<0-64> is policy name.

Command mode

Router Configuration mode.

Comments? infodev@avaya.com

area

Use this command to create and configure an OSPF area.

Syntax

```
area <ipaddr>
```

Variable definitions

Use the following table to use the **`area <ipaddr>`** command:

Variable	Value
<ipaddr> import [external|noexternal|nssa]	Set particular area as stub or nssa or normal area. <ipaddr> is area ID. [external| noexternal|nssa] is area type.
1.1.1.1 import-summaries enable	Enable import-summaries on particular area.
1.1.1.1 stub-metric <0-16777215>	Set stub-metric on particular area. <0-16777215> is stub metric value.
range <ipaddr> <ipaddr/x | ipaddr/x.x.x.x | default> [summary-link|nssa-extlink] [advertise-metric <0-65535>|advertise-mode [summarize|suppress|no-summarize]]	Creates an OSPF area range with the specified IP address and advertising mode. <ipaddr> is area ID. <ipaddr/x | ipaddr/x.x.x.x | default> is ip range. [summary-link|nssa-extlink] is lsa type. <0-65535> is metric value. [summarize|suppress|no-summarize] is advertise.
virtual-interface <ipaddr> <ipaddr>	Creates a virtual interface area identifier. <ipaddr> is area ID. <ipaddr> is router ID.
virtual-interface message-digest-key <ipaddr> <ipaddr> <1-255> md5-key WORD<1-16>	Adds an md5 key to the virtual interface. At most, two md5 keys can be configured to an interface. Multiple md5 key configurations are used for md5 transitions without bringing down an interface. <ipaddr> is area ID. <ipaddr> is virtual-interface ID. <1-255> is key ID. WORD<1-16> is md5 key.

To set an OSPF area configuration to a default condition, precede the command with the word `default.`

Example:

```
default area <ipaddr>
```

To cancel or delete an OSPF area configuration, precede the command with the word no.

Example:

```
no area <ipaddr>
```

Command mode

Router Configuration mode.

as-boundary-router enable

Use this command to enable OSPF Autonomous System boundary router:

Syntax

```
as-boundary-router enable
```

Command mode

Router Configuration mode.

default as-boundary-router enable

Use this command to set default OSPF Autonomous System boundary router.

Syntax

```
default as-boundary-router enable
```

Command mode

Router Configuration mode.

no as-boundary-router enable

Use this command to cancel or delete OSPF Autonomous System boundary router.

Syntax

```
no as-boundary-router enable
```

Command mode

Router Configuration mode.

auto-vlink enable

Use this command to enable OSPF auto-vlink.

Syntax

```
auto-vlink enable
```

To set OSPF auto-vlink to a default condition, use the following command:

```
default auto-vlink enable
```

To cancel or delete OSPF auto-vlink, use the following command:

```
no auto-vlink enable
```

Command mode

Router Configuration mode.

default-metric

Use this command to set the value of the default metric to apply to routes imported into the RIP domain.

Syntax

`default-metric` <*metric*>

Important:

You cannot assign a value of 0 to the default import metric. Entering the command **`default-metric 0`** deconfigures this parameter and restores the default value of 8.

Variable definitions

Use the following table to help you use the **`default-metric`** <*metric*> command.

Variable	Value
<*metric*>	Specifies the integer value with a range of 0 to 15. The default is 8.

Command mode

Router Configuration mode

default default-metric

The default import metric is the metric used for routes not learned through RIP if a route policy does not specify a metric for a particular protocol, such as OSPF. This command allows you to return the default import metric to its default value of 8.

Syntax

```
default default-metric
```

or

```
default-metric 0
```

Command mode

Router Configuration mode

default timer basic

This command allows you to return global timer parameters to their default values, use the following command:

Syntax

```
default timer basic
```

Variable definitions

Use the following table to help you use the **`default timer basic`** command.

Variable	Value
holddown	Resets the RIP holddown timer to its default value of 120 seconds on all the interfaces. The value of the holddown timer is the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable.
timeout	Resets the RIP timeout timer to its default value on all the interfaces. The default value is set indirectly by the global update time parameter. By default, the timeout timer is set at 6 times the update timer, in accordance with the RFC specification. With a default global update parameter setting of 30 seconds, the default timeout interval is 180 seconds.

Variable	Value
update	Resets the RIP update timer to its default value of 30 seconds. The value of the update timer is the time interval (in seconds) between regular RIP updates.

Command mode

Router Configuration mode

host-route

This command configures OSPF host-route parameters:

Syntax

`host-route <ipaddr>`

Variable definitions

Use the following table to help you use the **`host-route <ipaddr>`** command.

Variable	Value
area <ipaddr>	<ipaddr> is the area id.
<ipaddr> metric <0-65535>	Creates an OSPF host route for the IP address and sets the metric (cost) for the host route. <ipaddr> is ip address <0-65535> is metric value.

Command mode

Router Configuration mode.

interface loopback

The commands to configure CLIP are in the loopback interface configuration mode. This command allows you to access the loopback interface configuration mode.

Syntax

`interface loopback` *<id>*

Variable definitions

Use the following table to help you use the **`interface loopback`** *<id>* command.

Variable	Value
<*id*>	Specifies integer you assign to identify the CLIP interface. The range is 1 to 32.

Important:
You can configure a maximum of 32 CLIP interfaces on each device.

Command mode

Loopback interface configuration mode

ip address

This command allows you to create a CLIP interface in loopback interface configuration mode.

Syntax

`ip address [id` <*id*> **`]`**

Variable definitions

Use the following table to help you use the **`ip address [id`** <*id*> **`]`** command.

Variable	Value
<*ipaddr*>	The IP address of the CLIP interface.
<*id*>	Specifies integer you assign to identify the CLIP interface. The range is 1 to 32.

Command mode

Interface configuration mode

no ip address

This command allows you to delete a CLIP interface.

Syntax

`no ip address <addr>`

Command mode

Interface configuration mode

ip alternative-route

Use this command to enable alternative routing in the Ethernet Routing Switch 8300. The alternative route feature allows fast convergence to an alternative route in those cases when the primary route is unavailable. By default, alternative routing is enabled in the Ethernet Routing Switch 8300, thus allowing re-routing to an alternative link.

Syntax

```
ip alternative-route
```

Command mode

Global configuration mode

no ip alternative-route

Use this command to disable alternative routing in the Ethernet Routing Switch 8300.

Syntax

```
no ip alternative-route
```

Command mode

Global configuration mode

ip arp

Use this command to add a static entry to the Address Resolution Protocol (ARP) table on the Ethernet Routing Switch 8300.

Syntax

`ip arp` *[multicast-mac-flooding <enable>] [static-mcast <macaddr>] [timeout <value>] [<ipaddr> <macaddr> <slot/port> <vid>]*

Variable definitions

Use the following table to help you use the **`ip arp`** *[multicast-mac-flooding <enable>] [static-mcast <macaddr>] [timeout <value>] <ipaddr> <macaddr> <slot/port> <vid>* command.

Variable	Value
multicast-mac-flooding <enable>	Enables multicast MAC flooding.

Variable	Value
static-mcast <macaddr>	Adds a static multicast MAC Address entry.
timeout <value>	Sets the ARP entries lifetime aging period. Valid values here range from 1-32767 minutes.
<ipaddr> <macaddr> <slot/port <vid>>	Adds a static ARP entry to the specified IP address, MAC address, slot/port, or VLAN ID. **Important:** An IP address must be assigned to a VLAN before a static ARP entry can be associated with it.

Command mode

Global configuration mode

no ip arp

Use this command to remove a static entry from the Address Resolution Protocol (ARP) table on the Ethernet Routing Switch 8300.

Syntax

`no ip arp` *[multicast-mac-flooding <enable>] [static-mcast <macaddr>] <ipaddr>*

Variable definitions

Use the following table to help you use the **`no ip arp`** *[multicast-mac-flooding <enable>] [static-mcast <macaddr>] [<ipaddr>]* command.

Variable	Value
<ipaddr>	Specifies the IP address in dotted decimal notation {a.b.c.d.}.
multicast-mac-flooding <enable>	Disables multicast MAC flooding.
static-mcast <macaddr>	Removes a static multicast MAC Address entry.

Command mode

Global configuration mode

Comments? infodev@avaya.com

ip arp proxy

Use this command to enable proxy ARP on a VLAN.

Syntax

```
ip arp proxy
```

Command mode

Interface VLAN mode

no ip arp proxy

Use this command to disable proxy ARP on a VLAN.

Syntax

```
no ip arp proxy
```

Command mode

Interface VLAN mode

ip arp response

Use this command to enable ARP response.

Syntax

```
ip arp response
```

Command mode

Interface VLAN mode

no ip arp response

Use this command to disable ARP response

Syntax

```
no ip arp response
```

Command mode

Interface VLAN mode

ip default-ttl

Use this command to set the default time-to-live (ttl) value for a routed packet.

Syntax

`ip default-ttl` *<seconds>*

Variable definitions

Use the following table to help you use the command.

Variable	Value
<seconds>	Specifies the maximum number of seconds between 1 and 255 before a packet is discarded. The default value of 255 is inserted in the ttl field whenever one is not supplied.

Command mode

Global configuration mode

ip dhcp-relay broadcast

Use this command to enable dhcp-relay broadcasting.

Syntax

`ip dhcp-relay broadcast <enable|disable>`

Variable definitions

Use the following table to help you use the **`ip dhcp-relay broadcast <enable|disable>`** command.

Variable	Value
broadcast	Sends the server reply as a broadcast to the end station. After you disable broadcast, the switch sends the server reply as a unicast to the end station. The no form of this command is *no ip dhcp-relay*. The default form of this

Variable	Value
	command is default *ip dhcp-relay* broadcast.
ipaddr	Specifies the forwarding destination for this port protocol. You can enter either a specific server IP address, or an IP limited broadcast in dotted-decimal notation {a.b.c.d}.
listid	Specifies the UDP forwarding policy ID to delete.

Command mode

Interface VLAN mode

ip dhcp-relay

Use this command to enable dhcp-relay.

Syntax

```
ip dhcp-relay <enable|disable>
```

Command mode

Interface VLAN mode

ip dhcp-relay max-hop

Use this command to specify the value for the dhcp-relay max-hop.

Syntax

```
ip dhcp-relay max-hop <max-hop>
```

Variable definitions

Use the following table to help you use the **`ip dhcp-relay max-hop <max-hop>`**command.

Variable	Value
`<max-hop>`	Specifies the max-hop count. The range is 1-16.

Command mode

Interface VLAN mode

ip dhcp-relay min-sec

Use this command to specify the minutes and seconds of dhcp-relay.

Syntax

```
ip dhcp-relay min-sec <min-sec>
```

Variable definitions

Use the following table to help you use the **`ip dhcp-relay min-sec <min-sec>`**command.

Variable	Value
`<min-sec>`	Specifies the seconds count. The range is 1-65535.

Command mode

Interface VLAN mode

ip dhcp-relay mode

Use this command to specify the dhcp-relay mode.

Syntax

```
config interface vlan ip dhcp-relay mode <bootp|dhcp|bootp_dhcp>
```

Command mode

Interface VLAN mode

ip dhcp-relay fwd-path

Use this command to specify the dhcp-relay mode.

Syntax

```
ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D>
```

Variable definitions

Use the following table to help you use the **`ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D>`** command.

Comments? infodev@avaya.com

Variable	Value
<A.B.C.D> <A.B.C.D>	Specifies the IP addresses on an interface and of the DNCP server on the network. • The first A.B.C.D is the IP address configured on an interface (a locally configured IP address) that must be configured to forward or relay bootp or DHCP. • The second A.B.C.D is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out the interface.
<cr>	Creates the forwarding path from the client to the server.
disable	Disables DHCP relaying on the path from the IP address to the server. Disabled is the default.
enable	Enables DHCP relaying on the path from the IP address to the server.
mode <bootp|bootp-dhcp|dhcp>	Modifies DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both. *mode <bootp|bootp-dhcp|dhcp>*.

Command mode

Global Configuration mode or the VRF Router mode

ip ipfix (global)

Use this command to enable and configure IPFIX globally.

Syntax

`ip ipfix`

Variable definitions

The following table describes optional parameters that you enter after the **`ip ipfix`** command.

Variable	Value
active-timeout	Flow record of active time out value in minutes. The range is 1 to 60.
aging-interval	Flow record of aging interval in seconds. The range is 10 to 3600.
collector <ipaddr>	Configures or modifies a collector. <ipaddr> is the IP address of the collector.
enable	Enables ip ipfix.
export-interval	Configures the frequency interval of flow export to collector. The range is 10 to 3600 seconds.
exporter-enable	Enables the exporter state.
templated-refresh-interval	Configures the value of template refresh interval. The range is 300 to 3600 seconds.
templated-refresh-packets	Sets the value of template refresh packets. The range is 10000-100000.

Command mode

Global Configuration mode

no ip ipfix enable

Use this command to disable IPFIX globally.

Syntax

`no ip ipfix enable`

Command mode

Global Configuration mode

no ip ipfix collector

Use this command to remove or disable a collector IP address.

Syntax

`no ip ipfix collector <ipaddr>`

`<ipaddr>` identifies the collector IP address.

Comments? infodev@avaya.com

Variable definitions

The following table describes variables that you enter after the **no ip ipfix collector <ipaddr>** command.

Variable	Value
<cr>	Removes the collector IP address.
enable	Disables the collector IP address.

Command mode

Global Configuration mode

no ip ipfix exporter-enable

Use this command to disable the exporter state.

Syntax

no ip ipfix exporter-enable

Command mode

Global Configuration mode

ip ipfix (port)

Use this command to enable port-based IPFIX.

Syntax

ip ipfix

Variable definitions

The following table describes optional parameters that you enter after the **ip ipfix** command.

Variable	Value
enable	Enables ip ipfix on the accessed port.
port <PT_ETHPORTS> enable	Enables ip ipfix on a port or list of ports. <PT_ETHPORTS> lists one or more ports in the format; {slot/port[-slot/port][,....]}.

Command mode

Interface configuration mode

no ip ipfix (port)

Use this command to disable port-based IPFIX.

Syntax

`no ip ipfix`

Variable definitions

The following table describes optional parameters that you enter after the **`no ip ipfix`** command.

Variable	Value
enable	Disables ip ipfix on the accessed port.
port <PT_ETHPORTS> enable	Disables ip ipfix on a port or list of ports. <PT_ETHPORTS> lists one or more ports in the format; {slot/port[-slot/port][,....]}.

Command mode

Interface configuration mode

clear ip ipfix stats

Use this command to clear IPFIX exporter statistics.

Syntax

`clear ip ipfix stats`

Command mode

Global or Interface Configuration mode

ip forward-protocol udp

A UDP forwarding protocol specifies which port to watch for incoming UDP broadcasts, as well as the protocol name for that port.

Use this command to create a UDP forwarding protocol.

Syntax

`ip forward-protocol udp` <*updport*> <*protoname*>

Variable definitions

Use the following table to help you use the **`ip forward-protocol udp`** <*updport*> <*protoname*> command.

Variable	Value
updport	Specifies an integer value with a range of 1 to 65535.
protoname	Specifies string length {1..15}.

Command mode

Global configuration mode

no ip forward-protocol udp

This command allows you to delete a UDP protocol, use the following command in Global Config mode:

Syntax

`no ip forward-protocol udp` <*updport*>

Variable definitions

Use the following table to help you use the **`no ip forward-protocol udp`** <*updport*> command.

Variable	Value
updport	Specifies the port protocol to delete.

Command mode

Global configuration mode

ip forward-protocol udp portfwdlist

A UDP forwarding policy is a list of one or more UDP protocols that are assigned a forwarding IP address. Each forwarding policy also has a unique name and number. You can repeat this

command to add additional UDP protocols to an existing policy, to add another forwarding IP address for an existing UDP protocol, or to update the policy name.

Use this command to create a UDP forwarding policy.

Syntax

`ip forward-protocol udp portfwdlist` <*listid*> <*updport*> <*ipaddr*> **[** <*name*> **]**

Variable definitions

Use the following table to help you use the **`no ip forward-protocol udp`** <*updport*> command.

Variable	Value
updport	Specifies an integer value with a range of 1 to 65535. This port must have a defined UDP protocol.
ipaddr	Specifies the forwarding destination. You can enter either a specific server IP address, or an IP limited broadcast in dotted-decimal notation {a.b.c.d}.
listid	Specifies integer value from 1 to 1000. This provides a unique identifier for the UDP forwarding policy.
name	Specifies string length {1..15} used to describe the forwarding policy. If no value is entered when creating a new UDP forwarding policy, they system generates a name automatically.

Command mode

Global configuration mode

no ip forward-protocol udp portfwdlist

Use this command to delete an entire UDP forwarding policy.

Syntax

`no ip forward-protocol udp portfwdlist` <*listid*>

Variable definitions

Use the following table to help you use the **`no ip forward-protocol udp portfwdlist`** <*listid*> command.

Comments? infodev@avaya.com

Variable	Value
updport	Specifies the port protocol to remove.
ipaddr	Specifies the forwarding destination for this port protocol. You can enter either a specific server IP address, or an IP limited broadcast in dotted-decimal notation {a.b.c.d}.
listid	Specifies the UDP forwarding policy ID to delete.

Command mode

Global configuration mode

ip forward-protocol udp

Use this command to apply a UDP forwarding policy, to set the broadcast mask, and to set maximum TTL value for this interface.

Syntax

`ip forward-protocol udp [vlan` <*vlan*> **`]`**

Variable definitions

Use the following table to help you use the **`ip forward-protocol udp [vlan`** <*vlan*> **`]`** command.

Variable	Value
<*vlan*>	Specifies an optional integer with a range of 1 to 4000, specifying a particular VLAN on this interface to apply the specified settings.

The following table describes variables that you enter in the **`ip forward-protocol udp [vlan`** <*vlan*> **`]`** command.

Variable	Value
portfwdlist <*listid*>	Apply the specified UDP forwarding policy to this interface, and (optionally) set the broadcast mask for this interface and the maximum TTL value. *listid* is an integer with a range of 1 to 1000.

Variable	Value
broadcastmask <*mask*>	Set the broadcast mask for this interface, and (optionally) set the maximum TTL value. *mask* is the subnet mask in A.B.C.D format.
maxttl <*maxttl*>	Set the maximum TTL value for this interface. *maxttl* is an integer value with a range of 1 to 16. The default value is 4.

Command mode

Interface configuration mode

no ip forward-protocol udp

Use this command to remove UDP forwarding policies from an interface.

Syntax

`no ip forward-protocol udp [vlan` <*vlan*> **`] [portfwdlist`** <*listid*> **`] [broadcastmask`** <*mask*> **`]`**

If no optional parameters are included with this command, then all UDP forwarding policies are removed from the interface being configured.

Variable definitions

Use the following table to help you use the **`no ip forward-protocol udp [vlan`** <*vlan*> **`] [portfwdlist`** <*listid*> **`] [broadcastmask`** <*mask*> **`]`** command.

Variable	Value
mask	Specifies the subnet mask to remove.
listid	Specifies the UDP forwarding policy ID to remove.
vlan	Specifies a particular VLAN to remove the UDP forwarding policy from.

Command mode

Interface configuration mode

Comments? infodev@avaya.com

ip icmp-unreach-msg

Use this command to enable the Internet Control Message Protocol (ICMP) unreachable message. When enabled, this command allows the generation of ICMP net unreachable messages if the destination network is not reachable from this switch. These messages assist in determining if the routing switch is reachable over the network.

Syntax

```
ip icmp-unreach-msg
```

Command mode

Global configuration mode

no ip icmp-unreach-msg

Use this command to disable the ICMP unreachable message.

Syntax

```
no ip icmp-unreach-msg
```

Command mode

Global configuration mode

ip irdp enable

By default, router discovery is disabled. Use this command to enable router discovery.

Syntax

```
ip irdp enable
```

Command mode

Global configuration mode

no ip irdp enable

Use this command to disable router discovery.

Syntax

```
no ip irdp enable
```

Command mode

Global configuration mode

ip irdp

Use this command to enable router discovery.

Syntax

```
ip irdp
```

Variable definitions

Use the following table to help you use the **`ip irdp`** command.

Variable	Value
address <A.B.C.D>	Specifies the route discovery advertisement address.
holdtime <value>	Specifies the holdtime for router advertisements.
maxadvertinterval <value>	Specifies the Maximum Advertisement interval for router advertisements.
minadvertinterval <value>	Specifies the Minimum Advertisement interval for router advertisements.
multicast	Enables router discovery by setting the advertise flag to true.
preference <value>	Specifies the preference level for router advertisement.

Command mode

Global configuration mode

no ip irdp

Use this command to disable router discovery.

Syntax

```
no ip irdp
```


Comments? infodev@avaya.com

Command mode

Global configuration mode

default ip irdp

Use this command to set the router discovery to default values.

Syntax

```
default ip irdp
```

Command mode

Global configuration mode

no ip irdp multicast

Use this command to disable router discovery on VLANs.

Syntax

```
no ip irdp multicast
```

Command mode

Interface VLAN mode

ip irdp vlan multicast

Use this command to enable router discovery on a selected VLAN.

Syntax

```
ip irdp vlan <vid> multicast
```

Variable definitions

Use the following table to help you use the **`ip irdp vlan <vid> multicast`** command.

Variable	Value
`<vid>`	Specifies the ID of the selected VLAN.

Command mode

Interface VLAN mode

no ip irdp vlan multicast

Use this command toe disable router discovery on a specific VLAN.

Syntax

```
no ip irdp vlan <vid> multicast
```

Variable definitions

Use the following table to help you use the **`no ip irdp vlan <vid> multicast`** command.

Variable	Value
`<vid>`	Specifies the ID of the selected VLAN.

Command mode

Interface VLAN mode

ip more-specific-non-local-route enable

This command enables static routes to networks that are not directly connected. When enabled, this command allows a more specific non-local route to go into the routing table. The default is disabled.

Syntax

```
ip more-specific-non-local-route enable
```

Command mode

Global configuration mode

no ip more-specific-non-local-route enable

This command allows you to disable that feature that permits a more specific non-local route to go into the routing table.

Syntax

```
no ip more-specific-non-local-route enable
```

Command mode

Global configuration mode

ip ospf

This command configures OSPF on an interface:

Syntax

```
ip ospf
```

Variable definitions

Use the following table to help you use the **`ip ospf`** command.

Variable	Value
advertise-when-down enable	The network on this interface is advertised as up, even if no ports in the VLAN are active
area<*ipaddr*>	Set the vlan interface in a particular area. <ipaddr> is area ID.
authentication-key WORD<*0-8*>	Set the authentication key for the VLAN. WORD<0-8> is simple authentication key.
authentication-type [message-digest|none|simple]	Set the OSPF authentication type for the VLAN. [message-digest|none|simple] is authentication type.
authentication-key WORD<*0-2147483647*>	Set the OSPF dead interval for the VLAN. The dead interval is the number of seconds the switch's OSPF neighbors should wait before assuming that this OSPF router is down. PT_LONG<0-2147483647> is dead-interval value
enable	Enables OSPF on the VLAN.
hello-interval <*1-65535*>	Set the OSPF hello interval for the VLAN. The hello interval is the number of seconds between hello packets sent on this VLAN. <1-65535> is hello-interval value
interface-type [broadcast|passive]	Set the interface type, default is broadcast. A passive interface will not form neigborship with other routers. [broadcast|passive] is interface type.
message-digest-key <*1-255*>md5-key WORD<*0-16*>	Set the authentication message-digest-key for the VLAN. <1-255> is message-digest-key ID WORD<0-16> is md5 key

Variable	Value
metric <*1-65535*>	Set the OSPF metric for the VLAN. The switch advertises the metric in router link advertisements. <1-65535> is metric value
primary-md5-key <*1-255*>	Set primary message-digest-key. <1-255> is message-digest-key ID
priority <*0-255*>	Set the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If the priority is 0, the VLAN cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. <0-255> is priority value
retransmit-interval <*0-3600*>	Set the retransmit interval for the virtual interface. The retransmit interval is the number of seconds between link-state advertisement retransmissions. <0-3600> is retransmit interval value
transit-delay <*0-3600*>	Sets the transmit delay for the virtual interface. The transmit delay is the estimated number of seconds it takes to transmit a link-state update over the interface. <0-3600> is transit delay value
vlan<*1-4094*>	Set ospf configuration on paticular vlan. <1-4094> is the vlan ID.

Command mode

Interface configuration mode

ip ospf spf-run

This command forces an OSPF SPF run:

Syntax

```
ip ospf spf-run
```

Command mode

User Exec mode

Comments? infodev@avaya.com

ip prefix-list

The prefix list is a list of networks used by route policies to define an action. You can create one or more IP prefix lists and apply that list to any IP route policy.

When you configure the ge (mask length from) field to be less than the le (mask length to) field, it can also be used as a range.

This command allows you to configure a prefix list.

Syntax

`ip prefix-list` <*prefix-list name*>

Variable definitions

Use the following table to help you use the **`ip prefix-list`** <*prefix-list name*> command.

Variable	Value
prefix-list name	Specifies string length {1..64} that indicates the name of the prefix list.
<*ipaddr/mask*> [ge <*value*>] [le <*value*>]	Adds a prefix entry to the prefix list. Creates the prefix list if it does not already exist. • *ipaddr/mask* {a.b.c.d/x|a.b.c.d/x.x.x.x| default} is the IP address and network mask. • ge <*value*> is the lower bound of the mask length, where *value* is an integer value with a range of 0 to 32. The default is the mask length. • le <*value*> is the higher bound of the mask length, where *value* is an integer value with a range of 0 to 32. The default is the mask length. **Important:** Lower bound and higher bound mask lengths together can define a range of networks
name <*name*>	Renames the prefix list specified in the command. *name* is a string length {1..64}.

Command mode

Global configuration mode

no ip prefix-list

This command allows you to delete a prefix list.

Syntax

no ip prefix-list *<prefix-list name>*

Command mode

Global configuration mode

ip routing

Use this command to enable IP routing on the Ethernet Routing Switch 8300. By default, IP routing is enabled.

Syntax

`ip routing`

Command mode

Global configuration mode

no ip routing

Use this command to disable IP routing on the Ethernet Routing Switch 8300.

Syntax

`no ip routing`

Command mode

Global configuration mode

ip rip

Use this command to configure RIP on a specified VLAN interface.

Syntax

```
ip rip
```

Variable definitions

Use the following table to help you use the **`ip rip`** command.

Variable	Value
advertise-when-down <enable|disable>	If enabled, the network on this interface will be advertised as up, even if the VLAN is down. The default is disabled. When you configure a VLAN without any link and enable advertise-when-down, it will not advertise your route until the VLAN is active. Then the route is advertised even when the link is down. To disable advertising based on link status, disable this parameter.
auto-summary <enable|disable>	Enables or disables automatic route aggregation on the interface. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a network of a different class. The default is disabled. Routes with different metrics can be aggregated. RIP uses the out metric associated with the first route found in the routing table that is to be aggregated.
cost <*cost*>	Sets the RIP cost for this interface. *cost* is an integer value with a range of 1 to 15. The default value is 1.
default-listen <enable|disable>	Configures whether or not the interface will listen for RIP updates for the default route learned through RIP. The default is disabled.
default-supply <enable|disable>	Configures whether or not the interface will send RIP advertisements for the default route, if one exists in the routing table. The default is disabled.
domain <*domain*>	Specifies the value inserted into the Routing Domain field of all RIP packets sent on this interface. *domain* is an integer value with a range of 0 to 65535. The default is 0.
holddown <*seconds*>	Sets the RIP holddown timer for the interface. The value of the holddown timer is

Variable	Value
	the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable. *seconds* is an integer value with a range of 0 to 360. The default value is set by the global holddown parameter, which has a default of 120 seconds. The interface timer setting overrides the global parameter. However, if you subsequently reset the global parameter, the global setting then overrides the interface timer setting.
in-policy <*policy name*>	Sets the RIP policy for inbound filtering on the interface. The in-policy determines which routes will be learned on the interface. *policy name* is a string length {0..64}. To delete the policy, enter an empty string.
listen <enable|disable>	Configures whether or not the interface will listen for RIP routes. The default is enabled.
out-policy <*policy name*>	Sets the RIP policy for outbound filtering on the interface. The out-policy determines which routes will be advertised from the routing table on the interface. *policy name* is a string length {0..64}. To delete the policy, enter an empty string.
poison <enable|disable>	Sets whether or not RIP routes on the interface learned from a neighbor are advertised back to the neighbor. • If disabled, split horizon is invoked, and IP routes learned from an immediate neighbor are not advertised back to the neighbor. • If enabled, the RIP updates sent to a neighbor from which a route is learned are "poisoned" with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. The default is disabled.

Comments? infodev@avaya.com

Variable	Value
receive version <*version*>	Indicates which version of RIP updates the router will accept for this interface. The options for *version* are: • *rip1* — RIP version 1 (complies with RFC 1058). • *rip2* — RIP version 2 (complies with RFC 2453). • *rip1orrip2* — both versions of RIP. The default is *rip1orrip2*.
send version <*version*>	Indicates which version of RIP updates the router sends on this interface. The options for *version* are: • *notsend* — no updates are sent. • *rip1* — RIP version 1 (complies with RFC 1058; updates are broadcast). • *rip1comp* — compatible with RIP version 1 (RIP version 2 updates are broadcast using RFC 1058 route subsumption rules). • *rip2* — RIP version 2 (complies with RFC 2453; updates are multicast). The default is *rip1comp*.
supply <enable|disable>	Enables or disables the interface to supply RIP updates.
timeout <*seconds*>	Sets the RIP timeout interval for the interface. *seconds* is an integer value with a range of 15 to 259200. The default value is set indirectly by the global update time parameter. By default, the timeout timer is set at 6 times the update timer, in accordance with the RFC specification. With a default global update timer setting of 30 seconds, the default timeout interval is 180 seconds. Configure the timeout parameter on the interface only if you want to break the relationship with the update timer. For example, if you have set the global update parameter to a very short interval in order to minimize the problem of fast convergence, the associated default timeout may be too

Variable	Value
	short. In this case, configure the timeout interval manually. The interface timer setting overrides the global parameter. However, if you subsequently reset the global parameter, the global setting then overrides the interface timer setting. The timeout interval must be greater than the global update time parameter.
triggered <enable|disable>	Enables or disables automatic triggered updates for RIP on this interface. The default is disabled.

Command mode

Interface configuration mode

ip route

Use this command to create a new static route. You create static routes in order to route traffic from the Ethernet Routing Switch 8300 to other devices in the network, like an Ethernet Routing Switch 8300.

Syntax

`ip route [route] [mask] [next-hop] [cost] preference` <*value*> <*enable* | *disable]*<*weight*>

Variable definitions

Use the following table to help you use the **`ip route [route] [mask] [next-hop] [cost] preference`** <*value*> <*enable* | *disable]*<*weight*> command.

Variable	Value
[route] [mask] [next-hop] [cost]	Adds a static or default route to the switch. route/mask is the IP address and mask for the route's destination. next-hop <value> is the IP address of the next hop router; the next router at which packets must arrive on this route. cost <value> is the metric of the route. Valid values here are from 1-65535.
preference <*value*>	preference <value> specifies the route preference value assigned to the routes. Valid values range from 1-255, with a default of 1.

Comments? infodev@avaya.com

Variable	Value
<enable|disable>	Enables or disables the route.
<*weight*>	Specifies the route weight. Valid values range from 1-255.

Command mode

Global configuration mode

no ip route

Use this command to delete a static route.

Syntax

`no ip route [route] [mask] [next-hop` <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`no ip route [route] [mask] [next-hop`** <*value*> **`]`** command.

Variable	Value
`[route] [mask] [next-hop]`	Deletes a static or default route to the switch. route/mask is the IP address and mask for the route's destination. next-hop <value> is the IP address of the next hop router; the next router at which packets must arrive on this route.

Command mode

Global configuration mode

ip route preference protocol

Use this command to configure route preferences by protocol.

Syntax

`ip route preference protocol {static|rip}` <*value*>

where *value* is an integer value with a range of 0 to 255, indicating the preference. The value of 0 is reserved for local routes. If two protocols have the same configured value, the default value is used to break the tie. The default preference values are:

- local routes = 0
- static routes = 5
- RIP routes = 100

Variable definitions

The following table describes variables that you enter in the **`ip route preference protocol {static|rip}`** <*value*> command.

Variable	Value
ospf-intra	Specifies the protocol type OSPF-intra.
ospf-inter	Specifies the protocol type OSPF-inter.
ospf-extern1	Specifies the protocol type OSPF-extern1.
ospf-extern2	Specifies the protocol type OSPF-extern2.

Command mode

Global configuration mode

net6-mgmt ipv6

Use this command to configure route preferences ipv6 address to the management port.

Syntax

`net6-mgmt ipv6 <WORD 0–46> [cpu-slot<3-6>]`

Variable definitions

The following table describes variables that you enter in the **`net6-mgmt IPv6`** command.

Variable	Value
<WORD 0–46>	Specifies the IPv6 address and prefix length to assign to the management interface in the format IPv6address/prefix-length.
[cpu-slot<3-6>]	Specifies the cpu slot.

Command mode

Global configuration mode

Comments? infodev@avaya.com

no net6-mgmt ipv6

Use this command to delete IPv6 address.

Syntax

no net6-mgmt ipv6 <WORD 0–46> [cpu-slot<3-6>]

Variable definitions

The following table describes variables that you enter in the **no net6-mgmt IPv6 <WORD 0–46> [cpu-slot<3-6>]** command.

Variable	Value
<WORD 0–46>	Specifies the IPv6 address and prefix length to assign to the management interface in the format IPv6address/prefix-length.
[cpu-slot<3-6>]	Specifies the cpu slot.

Command mode

Global configuration mode

no net6-mgmt ipv6 route

Use this command to delete a management route

Syntax

no net6-mgmt ipv6 route <WORD 0–255> <WORD 0–255>

Variable definitions

The following table describes variables that you enter in the **no net6-mgmt IPv6 route <WORD 0–255> <WORD 0–255>** command.

Variable	Value
<WORD 0–255>	Specifies the net address and prefix length of the network to add.
<WORD 0–255>	Specifies the gateway IPv6 address.

Command mode

Global configuration mode

net6-mgmt ipv6 route

Use this command to configure a management route to establish communication between networks.

Syntax

net6-mgmt ipv6 route <WORD 0–255> <WORD 0–255>

Variable definitions

The following table describes variables that you enter in the **net6-mgmt IPv6 <WORD 0–255> <WORD 0–255>** command.

Variable	Value
<WORD 0–255>	Specifies the net address and prefix length of the network to add.
<WORD 0–255>	Specifies the gateway IPv6 address.

Command mode

Global configuration mode

ipv6 mgmt-virtual

Use this command to configure a virtual IPv6 address.

Syntax

ipv6 mgmt-virtual <WORD 0–46>

Variable definitions

The following table describes variables that you enter in the **net6-mgmt IPv6 <WORD 0–46>** command.

Variable	Value
<WORD 0–46>	Specifies the IPv6 address and prefix length to assign to the management interface in the format IPv6address/prefix-length.

Command mode

Global configuration mode

Comments? infodev@avaya.com

lldp

Use this command to set the LLDP transmission parameters.

Syntax

```
lldp [tx-interval <5-32768>] [tx-hold-multiplier <2-10>] [reinit-delay <1-10>] [tx-delay <1-8192>] [med-fast-start <1-10>]
```

Variable definitions

The following table describes variables that you enter after the **lldp** command.

Variable	Value
tx-interval <5-32768>	sets the global interval between successive transmission cycles (default value is 30)
tx-hold-multiplier <2-10>	sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV (default value is 4)
reinit-delay <1-10>	sets the delay for the reinitialization attempt if the adminStatus is disabled (default value is 2)
tx-delay <1-8192>	sets the minimum delay between successive LLDP frame transmissions (default value is 2)
med-fast-start <1-10>	sets the MED Fast Start repeat count value (default value is 3)

Command mode

Global configuration mode

default lldp

Use this command to set the LLDP transmission parameters to their default values. If no parameters are specified, the default lldp sets all parameters to their default parameters.

Syntax

```
default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-delay] [tx-delay] [med-fast-start]
```

Command mode

Global configuration mode

lldp port status

Use this command to set the LLDPU transmit and receive status on the ports.

rxonly: enables LLDPU receive only.

txAndRx: enables LLDPU transmit and receive.

txOnly: enables LLDPU transmit only. (default value is txAndRx)

Syntax

`lldp port <portlist> status {rxOnly | txAndRx | txOnly}`

Command mode

Interface configuration mode

no lldp port

Use this command to disable LLDP features on the port,

Syntax

`no lldp port <portlist> [status]`

Command mode

Interface configuration mode

default lldp port

This command sets the LLDP port parameters to their default values.

Syntax

`default lldp port <portlist> [status]`

Command mode

Interface configuration mode

Comments? infodev@avaya.com

lldp port status

This command sets the LLDPU transmit and receive status on the ports.

rxonly: enables LLDPU receive only.

txAndRx: enables LLDPU transmit and receive.

txOnly: enables LLDPU transmit only. (default value is txAndRx)

Syntax

```
lldp port <portlist> status {rxOnly | txAndRx | txOnly}
```

Command mode

Interface configuration mode

no lldp status

This command disables the LLDP features on the port.

Syntax

```
no lldp [status]
```

Command mode

Interface configuration mode

default lldp port

This command sets the LLDP port parameters to their default values.

Syntax

```
default lldp port <portlist> [status]
```

Command mode

Interface configuration mode

lldp tx-tlv

This command set the optional Management TLVs to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist> tx-tlv [port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]
```

Variable definitions

Use the following table to help you use the **`lldp [port <portlist> tx-tlv [port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]`** command.

Variable	Value
port-desc	port description TLV (default value is false: not included)
sys-name	system name TLV (default value is false: not included)
sys-desc	system description TLV (default value is false: not included)
sys-cap	system capabilities TLV (default value is false: not included)
local-mgmt-addr	local management address TLV (default value is false: not included)

Command mode

Interface configuration mode

no lldp tx-tlv

This command specifies the optional Management TLVs not to include in the transmitted LLDPDUs

Syntax

```
no lldp [port <portlist> tx-tlv [port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]
```

Command mode

Interface configuration mode

Comments? infodev@avaya.com

default lldp tx-tlv

This command sets the LLDP Management TLVs to their default values.

Syntax

```
default lldp [port <portlist> tx-tlv [port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]
```

Command mode

Interface configuration mode

lldp tx-tlv dot1

This command sets the optional IEEE 802.1 organizationally-specifc TLVs to be included in the transmitted LLDPDUs

Syntax

```
lldp [port <portlist> tx-tlv dot1 [port-vlan-id] [vlan-name] [port-protocol-vlan-id] [protocol-identity {EAP | LLDP | STP} ]
```

Variable definitions

Use the following table to help you use the **`lldp [port <portlist> tx-tlv dot1 [port-vlan-id] [vlan-name] [port-protocol-vlan-id] [protocol-identity {EAP | LLDP | STP} ]`** command.

Variable	Value
`port-vlan-id`	Port VLAN ID TLV (default value is false: not included)
`vlan-name`	VLAN Name TLV (default value is none)
`port-protocol-vlan-id`	Port and Protocol VLAN ID TLV (default value is none)
`protocol-identity {EAP | LLDP | STP}`	Protocol Identity TLV (default value is none)

Command mode

Interface configuration mode

no lldp tx-tlv dot1

This command specifies the optional IEEE 802.1 TLVs to exclude in the transmitted LLDPDUs.

Syntax

```
no lldp [port <portlist>] tx-tlv dot1 [port-vlan-id] [vlan-name]
[port-protocol-vlan-id] [protocol-identity { EAP | LLDP | STP } ]
```

Command mode

Interface configuration mode

default lldp tx-tlv dot1

This command resets the optional IEEE 802.1 organizationally-specifc TLVs to their default values.

Syntax

```
default lldp [port <portlist> ] tx-tlv dot1 [port-vlan-id] [vlan-
name ] [port-protocol-vlan-id] [protocol-identity {EAP | LLDP |
STP} ]
```

Command mode

Interface configuration mode

lldp tx-tlv dot3

This command specifies the optional IEEE 802.3 organizationally-specifc TLVs to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist> ] tx-tlv dot3 [mac-phy-config-status] [mdi-
power-support] [link-aggregation][maximum-frame-size]
```

Variable definitions

Use the following table to help you use the **`lldp [port <portlist> ] tx-tlv dot3 [mac-phy-config-status] [mdi-power-support] [link-aggregation] [maximum-frame-size]`** command.

Comments? infodev@avaya.com

Variable	Value
mac-phy-config-status	MAC/Phy Configuration/Status TLV (default value is false: not included)
mdi-power-support	Power Via MDI TLV (default value is false: not included)
link-aggregation	Link Aggregation TLV (default value is false: not included)
maximum-frame-size	Maximum Frame Size TLV (default value is false: not included)

Command mode

Interface configuration mode

no lldp tx-tlv dot3

This command specifies the optional IEEE 802.3 TLVs not to include in the transmitted LLDPDUs.

Syntax

```
no lldp [port <portlist> ] tx-tlv dot3 [mac-phy-config-status] [mdi-power-support] [link-aggregation] [maximum-frame-size]
```

Command mode

Interface configuration mode

default lldp tx-tlv dot3

This command sets the optional IEEE 802.3 organizationally-specifc TLVs to their default values.

Syntax

```
default lldp [port <portlist> ] tx-tlv dot3 [mac-phy-config-status] [mdi-power-support] [link-aggregation] [maximum-frame-size]
```

Command mode

Interface configuration mode

lldp tx-tlv med

This command specifies the optional organizationally-specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist> ] tx-tlv med [capabilities] [network-policy]
[location] [extendedPSE]
```

Variable definitions

Use the following table to help you use the **`lldp [port <portlist> ] tx-tlv med [capabilities] [network-policy] [location] [extendedPSE]`** command.

Variable	Value
`capabilities`	Enables MED capabilities TLV (default value is false: not included).
`extendedPSE`	Enables extended PSE TLV (default value is false: not included).
`location`	Enables location Identification TLV (default value is false: not included).
`network-policy`	Enables Network Policy TLV (default value is false: not included).

Command mode

Interface configuration mode

no lldp tx-tlv med

This command specifies the optional Management TLVs not to include in the transmitted LLDPDUs.

Syntax

```
no lldp [port <portlist> ] tx-tlv med [capabilites] [extendedPSE]
[location] [network-policy]
```

Command mode

Interface configuration mode

Comments? infodev@avaya.com

default lldp tx-tlv med

This command sets the optional organizationally-specifc TLVs for MED devices to their default values.

Syntax

```
default lldp [port <portlist> ] tx-tlv med [capabilities]
[extendedPSE] [location] [network-policy]
```

Command mode

Interface configuration mode

lldp location-identification civic-address

This command specifies LLDP civic address parameters. Note: The maximum total size for the civic-address TLV is 256 bytes. If this TLV is any larger, the ERS 8300 Series switch does not transmit it.

Syntax

```
lldp location-identification civic-address [country-code]
[additional-code] [additional-information] [apartment] [block]
[building] [city] [city-district ] [county] [floor] [house-number]
[house-number-suffix] [landmark] [leading-street-direction] [name]
[p.o.box] [place-type] [postal-community-name] [postal/zip-code]
[room-number] [state] [street] [street-suffix] [trailing-street-
suffix]
```

Variable definitions

Use the following table to help you use the command.

Variable	Value
country-code	Country code value
additional-code	Additional code
additional-information	Additional location information
apartment	Unit (apartment, suite)
block	Neighborhood, block
building	Building (structure)
city	City, township, shi (JP)

Variable	Value
city-district	City division, city district, ward
county	County, parish, gun (JP), district (IN)
floor	Floor
house-number	House number
house-number-suffix	House number suffix
landmark	Landmark or vanity address
leading-street-direction	Leading street direction
name	Residence and office occupant
pobox	Post office box
place-type	Office
postal-community-name	Postal community name
zip-code	Zip code
room-number	Room number
state	National subdivisions (state, canton, region)
street	Street
street-suffix	Street suffix
trailing-street-suffix	Trailing street suffix

Command mode

Interface configuration mode

manualtrigger ip rip interface vlan

Use this command to execute a manually triggered RIP update on a specified VLAN interface.

Syntax

manualtrigger ip rip interface vlan <*vid*>

Variable definitions

Use the following table to help you use the command.

Comments? infodev@avaya.com

Variable	Value
vid	Specifies the VLAN ID.

Command mode

User EXEC mode

network

In addition to being enabled globally on the switch, RIP must be enabled separately on each participating interface.

This command enables RIP on an interface.

Syntax

`network` <*ipaddr*>

Variable definitions

Use the following table to help you use the **`network <ipaddr>`** command.

Variable	Value
ipaddr	Indicates the IP address of the interface.

Command mode

Router Configuration mode

no network

Use this command to disable RIP on an interface.

Syntax

`no network` <*ipaddr*>

Variable definitions

Use the following table to help you use the **`no network <ipaddr>`** command.

Variable	Value
ipaddr	Indicates the IP address of the interface.

Command mode

Router Configuration mode

network area

This command sets an OSPF interface on a particular OSPF area:

Syntax

```
network <ipaddr> area <ipaddr>
```

where:

- <ipaddr> is interface network ip address.
- <ipaddr> is the area ID.

To set an OSPF interface on a particular OSPF area to a default condition, use the following command:

```
default network <ipaddr> area <ipaddr>
```

To cancel or delete an OSPF interface on a particular OSPF area, use the following command:

```
no network <ipaddr> area <ipaddr>
```

Command mode

Router Configuration mode.

redistribute enable

This command enables OSPF redistribution:

Syntax

```
redistribute enable
```

To set OSPF redistribution to a default condition, use the following command:

```
default redistribute enable
```

To cancel or delete OSPF redistribution, use the following command:

```
no redistribute enable
```

Command mode

Router Configuration mode.

Comments? infodev@avaya.com

redistribute source

This command creates OSPF redistribution from particular source, metric and type:

Syntax

```
redistribute source [direct|rip|static] [enable|metric <0-65535>|
metric-type [type1|type2|any]|route-policy WORD<0-64>| subnets
[allow|supress]]
```

where:

- [direct|rip|static] is source type
- <0-65535> is metric value
- [type1|type2|any] is metric type
- WORD<0-64> is policy name
- [allow|supress] is subnet redistribute type

To set OSPF redistribution from particular source, metric and type to a default condition, use the following command:

```
default redistribute source [direct|rip|static] [enable|metric
<0-65535>| metric-type [type1|type2|any]|route-policy WORD<0-64>|
subnets [allow|supress]]
```

To cancel or delete OSPF redistribution from particular source, metric and type,use the following command:

```
no redistribute source [direct|rip|static] [enable|metric <0-65535>|
metric-type [type1|type2|any]|route-policy WORD<0-64>| subnets
[allow|supress]]
```

Command mode

Router Configuration mode.

route-map

This command allows you to create a route policy and specify the action to be taken when a route policy is selected for a specific route.

Syntax

`route-map` <*policy name*>

Variable definitions

Use the following table to help you use the **`route-map <policy name>`** command.

Variable	Value
policy name	Specifies string length {0..64}indicating the name you assigned to the policy
<*seq number*>	Specifies the sequence number. The range is 1 to 65535.
permit [<*seq number*>]	Allows the route.
deny [<*seq number*>]	Denies the route.

The following table describes variables that you after the **`route-map <policy name> <seqnumber>`** command.

Variable	Value
enable	Enables the route policy with the policy name and sequence number specified in the command.
match [interface <*prefix-list*>] [metric <*metric*>] [network <*prefix-list*>] [next-hop <*prefix-list*>] [protocol <*protocol name*>] [route-source <*prefix-list*>]	If configured, the switch matches the specified criterion: • interface <*prefix-list*> — matches the IP address of the received interface against the contents of the specified prefix list, where *prefix-list* is a string length {0..1027}. Applicable to RIP only. • metric <*metric*>— matches the metric of the incoming advertisement or existing route against the specified value, where *metric* is an integer value with a range of 0 to 65535. If 0, then this field is ignored. The default is 0. • network <*prefix-list*> — matches the destination network against the contents of the specified prefix list, where *prefix-list* is a string length {0..1027}. • next-hop <prefix-list> — matches the next hop IP address of the route against the contents of the specified prefix list, where *prefix-list* is a string length {0..1027}. • protocol <*protocol name*> — matches the protocol through which the route is learned, where protocol name {any|xxx} is a string length {0..40} and xxx is local|rip|static or any combination separated by | (vertical line). Used for RIP announce policies only. • route-source <*prefix-list*> — matches the source IP address for RIP routes against

Comments? infodev@avaya.com

Variable	Value
	the contents of the specified prefix list, where *prefix-list* is a string length {0..1027}. This field is ignored for all other route types.
name <*policy name*>	Renames a policy once it has been created. This command changes the name field for all sequence numbers under the given policy. *policy name* is a string length {0..64}.
set [injectlist <*prefix-list*>] [ip-preference <*pref-value*>] [mask <*ipaddr*>]	If configured, the switch sets the specified parameter: • injectlist <*prefix-list*> — replaces the destination network of the route that matches this policy with the contents of the specified prefix list, where *prefix-list* is a string length {0..1027}. • ip-preference <*pref-value*> — specifies the route preference value to be assigned to the route that matches this policy, where *pref-value* is an integer value with a range of 0 to 255. If 0, the global preference value is used. The default is 0. Used for accept policies only. • mask <*ipaddr*> — sets the mask of the route that matches this policy, where *ipaddr* is a valid contiguous IP mask. Used for RIP accept policies only.

Command mode

Global configuration mode

no route-map

This command allows to delete a route policy.

Syntax

no route-map <*policy name*> <*seq number*>

Variable definitions

Use the following table to help you use the **no route-map <policy name> <seq number>** command.

Variable	Value
seq number	Indicates the sequence number. The range is 1 to 65535.
policy name	Specifies string length {0..64} indicating the name assigned to the policy

Command mode

Global configuration mode

router ospf

This command allows you to enter Router Config mode for OSPF. Once in Router Config mode, you can configure OSPF global parameters:

Syntax

```
router ospf
```

Command mode

Global configuration mode

router ospf enable

This command enables OSPF globally on the switch

Syntax

```
router ospf enable
```

To disable OSPF globally on the switch, use the following command:

```
no router ospf enable
```

Command mode

Global configuration mode

no router ospf enable

This command disables OSPF globally on the switch

Syntax

```
no router ospf enable
```

Command mode

Global configuration mode

router rip

This command allows you to enter Router Config mode for RIP. Once in Router Config mode, you can configure the RIP global timer and default metric parameters:

Syntax

```
router rip
```

Command mode

Global configuration mode

router rip enable

This command enables RIP globally on the switch.

Syntax

`router rip enable`.

Command mode

Global configuration mode

no router rip enable

This command disables RIP globally on the switch.

Syntax

```
no router rip enable
```

Command mode

Global configuration mode

router-id

This command sets the OSPF router ID:

Syntax

```
router-id <ipaddr>
```

To set OSPF router ID to a default condition, use the following command:

```
default router-id <ipaddr>
```

<ipaddr> is the router ID.

To cancel or delete OSPF router ID, use the following command:

```
no router-id <ipaddr>
```

Command mode

Router Configuration mode

slpp

This command is used to configure Simple Loop Protection Protocol (SLPP).

Syntax

```
slpp
```

Variable definitions

Use the following table to help you use the **`slpp`** command.

Variable	Value
operation	Enables the SLPP operation.
ethertype *<1-65535|0x1-0xffff>*	Specifies the SLPP PDU ether type.Enter a value from 1 to 65535 in hexadecimal (0x8104) or decimal (33028) format. The default is 0x8104.
tx-interval *<500-5000>*	Sets the SLPP packet transmit interval. The range is 500 to 5000 ms, and the default is 500 ms.
vid *<1-4000>*	Adds VLANs to a SLPP transmission list. Enter a vlan id from 1-4000.

Command mode

Global configuration mode

Default slpp

Use this command to set the SLPP parameters to default.

Syntax

```
default slpp
```

Variable definitions

Use the following table to help you use the **`default slpp`** command.

Variable	Value
operation	Sets the SLPP operation to default: disable.
ethertype	Sets the SLPP PDU ether type to default: 0x8104.
tx-interval	Sets the SLPP packet transmit interval to default: 500 ms.

Command mode

Global configuration mode

no slpp

Use this command to disable SLPP parameters.

Syntax

```
no slpp
```

Variable definitions

Use the following table to help you use the **`no slpp`** command.

Variable	Value
<*cr*>	Indicates a carriage return.
operation	Disables the SLPP operation.
vid <*1-4000*>	Deletes VLANs from a SLPP transmission list. Enter a VLAN ID from 1-4000.

Command mode

Global configuration mode

slpp port

Use this command to configure SLPP on a port.

Syntax

```
slpp port [port <portlist>] [packet-rx ] [packet-rx-threshold]
```

Variable definitions

Use the following table to help you use the **`slpp port [port <portlist>] [packet-rx ] [packet-rx-threshold]`** command.

Variable	Value
<*portlist*>	Specifies the slot/port.
packet-rx	Enables SLPP packet reception on the listed ports.
packet-rx-threshold	Specifies the SLPP reception threshold on the ports. Enter a value from 1-500.

Command mode

Interface fastethernet or gigabitethernet mode

default slpp port

Use this command to set the SLPP parameters on a port to default.

Syntax

`default slpp [port`<*portlist*>**`][packet-rx ][packet-rx-threshold]`**

Variable definitions

Use the following table to help you use the **`default slpp [port`**<*portlist*>**`][packet-rx ] [packet-rx-threshold]`** command.

Variable	Value
portlist	Specifies the slot/port.
packet-rx	Sets the SLPP operation on the listed port or ports to default:disable

Variable	Value
packet-rx-threshold	Sets the SLPP PDU reception threshold on the ports to default: 1.

Command mode

Interface fastethernet or gigabitethernet mode

no slpp port

Use this command to cancel the configuration of SLPP parameters.

Syntax

`no slpp [port <portlist>] [packet-rx]`

Variable definitions

Use the following table to help you use the **`no slpp [port <portlist>] [packet-rx]`** command.

Variable	Value
<portlist>	Specifies the slot/port.
packet-rx	Disables SLPP packet reception on the listed ports.

Command mode

Interface fastethernet or gigabitethernet mode

spoof-detect

Use this command to enable IP spoof detection.

Syntax

`spoof-detect`

Variable definitions

The following table defines parameters that you enter after the **`spoof-detect`** command.

Variable	Value
enable	Enables spoof detection on the port.

Variable	Value
[port <portlist>]	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Interface Configuration mode

no spoof-detect

Use this command to disable IP spoof detection.

Syntax

no spoof-detect

Variable definitions

The following table defines parameters that you enter after the **no spoof-detect** command.

Variable	Value
enable	Disables spoof detection on the port.
[port <portlist>]	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Interface Configuration mode

show spoof-detect

Use this command to view IP spoof detection information.

Syntax

show spoof-detect

Variable definitions

The following table defines parameters that you enter after the **show spoof-detect** command.

Comments? infodev@avaya.com

Variable	Value
<portlist>	Specifies a single port or group of ports, entered as {slot/port[-slot/ port][,...]}.
<*vid*>	Identifies the VLAN. Values range from 1 to 4000.

Command mode

Privileged EXEC mode

timer basic

Use this command to set the global update, holddown, and timeout timers.

Syntax

`timer basic`

Variable definitions

Use the following table to help you use the **`timer basic`** command.

Variable	Value
holddown <*seconds*>	Sets the RIP holddown timer. The value of the holddown timer is the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable. *seconds* is an integer value with a range of 0 to 360. The default is 120 seconds. The global holddown parameter sets the value of the holddown timer for the VLAN interfaces, but you can override the value for a specific interface.
timeout <*seconds*>	Sets the RIP timeout interval. *seconds* is an integer value with a range of 15 to 259200. The default value is set indirectly by the global update time parameter. By default, the timeout timer is set at 6 times the update timer, in accordance with the RFC specification. With a default global update parameter setting of 30 seconds, the default timeout interval is 180 seconds. The default

Variable	Value
	global timeout setting changes when the global update time parameter is changed. Configure the timeout parameter only if you want to break the relationship with the update timer. For example, if you have set the global update parameter to a very short interval in order to minimize the problem of fast convergence, the associated default timeout may be too short. In this case, configure the timeout interval manually. The global timeout parameter sets the value of the timeout timer for the VLAN interfaces, but you can override the value for a specific interface .
update <*seconds*>	Sets the RIP update timer. The value of the update timer is the time interval (in seconds) between regular RIP updates. *seconds* is an integer value with a range of 1 to 2147483647. The default is 30 seconds. The global updatetime parameter sets the update timer for the VLAN interfaces. The updatetime value must be less than the timeout interval.

Command mode

Router Configuration mode

timers basic holddown

This command sets the OSPF holddown timer value:

Syntax

```
timers basic holddown <0-60>
```

where:

<0-60> is holddown timer value in seconds.

To set OSPF holddown timer value to a default value, use the following command in Router Config mode:

```
default timers basic holddown
```


Comments? infodev@avaya.com

Command mode

Router Configuration mode.

trap enable

This command enables OSPF traps:

Syntax

```
trap enable
```

To set OSPF trap to a default condition, use the following command in Router Config mode:

```
default trap enable
```

To disable OSPF traps, use the following command in Router Config mode:

```
no trap enable
```

Command mode

Router Configuration mode

vlan nlb-mode

Use this command to configure network load balancing (NLBS) on a specific VLAN.

Syntax

```
vlan nlb-mode <vid> <igmp-mcast|multicast|unicast>
```

Variable definitions

Use the following table to help you use the **`vlan nlb-mode <vid> <igmp-mcast|multicast|unicast>`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID from 1 to 4000
<disable|igmp-mcast|multicast|unicast>	Specifies the mode of the NLBS feature. NLBS must be in the disable mode, which is the default mode, before you can choose one of the other three modes.

Command mode

Global configuration mode

no vlan nlb-mode

Use this command to configure NLSB in disable mode.

Syntax

```
no vlan nlb-mode <vid>
```

Variable definitions

Use the following table to help you use the **`no vlan nlb-mode <vid>`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID from 1 to 4000.

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 10: Layer 2 and 3 operations commands

This chapter describes ACLI layer 2 and layer 3 operations commands and their parameters.

Navigation

- bcast-mcast-rate-limit enable on page 267
- ist on page 268
- no ist on page 268
- ist enable on page 269
- no ist enable on page 269
- no mlt encapsulation dot1q on page 269
- no mlt name on page 270
- interface mlt on page 270
- smlt on page 270
- no smlt on page 271
- ip rsmlt on page 271
- default ip rsmlt on page 272
- no ip rsmlt on page 272
- mlt members on page 272
- mlt add-vlan on page 273
- mlt name on page 273
- no mlt members on page 274
- mlt remove-vlan on page 274
- mlt create on page 275
- mlt encapsulation on page 275
- no mlt encapsulation on page 276
- no mlt on page 276
- spanning-tree stp on page 277

- spanning-tree stp add-ports on page 278
- spanning-tree stp create on page 278
- spanning-tree stp remove-ports on page 279
- no spanning-tree on page 279
- telnet-access on page 280
- vlan action on page 280
- vlan add-mlt on page 281
- vlan members on page 281
- vlan name on page 282
- vlan qos-level on page 283
- no vlan on page 283
- vlan create type port on page 284
- vlan create type protocol-ApltkEther2Snap on page 284
- vlan create type protocol-decEther2 on page 285
- vlan create type protocol-decOtherEther2 on page 286
- vlan create type protocol-ipEther2 on page 286
- vlan create type protocol-ipv6Ether2 on page 287
- vlan create type protocol-ipx802.2 on page 288
- vlan create type protocol-ipx802.3 on page 289
- vlan create type protocol-ipxEther2 on page 289
- vlan create type protocol-ipxSnap on page 290
- vlan create type protocol-Netbios on page 291
- vlan create type protocol-RarpEther2 on page 291
- vlan create type protocol-sna802.2 on page 292
- vlan create type protocol-snaEther2 on page 293
- vlan create type protocol-Userdef on page 294
- vlan create type protocol-vinesEther2 on page 294
- vlan create type protocol-xnsEther2 on page 295
- vlan fdb-entry aging-time on page 296
- vlan fdb-entry flush on page 296
- vlan fdb-entry qos-level on page 297
- vlan fdb-entry sync on page 297
- vlan fdb-filter add on page 298
- no vlan fdb-filter on page 299

- vlan fdb-static add on page 299
- no vlan fdb-static on page 300
- vlan static-mcastmac add on page 300
- vlan static-mcastmac add-mlt on page 301
- vlan static-mcastmac remove-mlt on page 301
- vlan static-mcastmac add-ports on page 302
- vlan static-mcastmac remove on page 302
- vlan static-mcastmac remove-mlt on page 303
- vlan static-mcastmac remove-ports on page 304
- no vlan static-mcastmac on page 304
- interface vlan on page 305
- ip address on page 305
- ip vrf on page 306
- vrf on page 306

bcast-mcast-rate-limit enable

This command enables rate limiting on a port.

Syntax

```
bcast-mcast-rate-limit {port <portlist>}<percent value> enable
```

Variable definitions

Use the following table to help you use the **`bcast-mcast-rate-limit {port <portlist>}<percent value> enable`** command.

Variable	Value
`port <portlist>`	Specifies the list of ports, on which you enable rate limiting.
`<percent value>`	Specifies the rate limit to use, expressed as a percentage. The value can be from 1-100.

Command mode

Interface configuration mode

ist

This command configures an IST MLT from an existing MLT.

Syntax

```
ist [enable|peer-ip <A.B.C.D> ]
```

Variable definitions

Use the following table to help you use the **`ist [enable|peer-ip <A.B.C.D> ]`** command.

Variable	Value
`enable`	Enables ist on an MLT interface.
`peer-ip <A.B.C.D>`	Specifies the peer IP address for the IST.

Command mode

MLT Interface Configuration mode

no ist

This command clears the IST configuration.

Syntax

```
no ist [enable|peer-ip]
```

Variable definitions

Use the following table to help you use the **`no ist [ip]`** command.

Variable	Value
`enable`	Disables ist on an MLT interface.
`[peer-ip]`	Specifies the peer IP address for the IST.

Command mode

MLT Interface Configuration mode

Comments? infodev@avaya.com

ist enable

This command enables the IST MLT.

Syntax

```
ist enable
```

Command mode

MLT Interface Configuration mode

no ist enable

This command disables the IST.

Syntax

```
no ist enable
```

Command mode

MLT Interface Configuration mode

no mlt encapsulation dot1q

This command removes encapsulation from a link aggregation group.

Syntax

```
no mlt <mid> encapsulation dot1q
```

Variable definitions

Use the following table to help you use the **`no mlt <mid> encapsulation dot1q`** command.

Variable	Value
<mid>	Specify a link aggregation group number from 1 to 31.

Command mode

Global configuration mode

no mlt name

This command removes a link aggregation group name.

Syntax

```
no mlt <mid> name
```

Variable definitions

Use the following table to help you use the **`no mlt <mid> name`** command.

Variable	Value
<mid>	Specify a link aggregation group number from 1 to 31.

Command mode

Global configuration mode

interface mlt

This command enters the MLT Interface Configuration command mode.

Syntax

```
interface mlt <1-31>
```

Variable definitions

Use the following table to help you use the **`interface mlt <1-31>`** command.

Variable	Value
`mlt`*<1-31>*	Specifies the ID of the MLT to configure.

Command mode

Global configuration mode

smlt

This command creates an SMLT from an existing MLT.

Syntax

```
smlt <1-512>
```

Variable definitions

Use the following table to help you use the **`smlt <1-512>`** command.

Variable	Value
`smlt`*<1-512>*	Specifies the SMLT ID.

Command mode

MLT Interface Configuration mode

no smlt

This command deletes the SMLT.

Syntax

```
no smlt
```

Command mode

MLT Interface Configuration mode

ip rsmlt

Use this command to configure RSMLT on each IP VLAN interface to obtain a rapid failover time. The IP routing protocol must be enabled on VLAN Layer 3 interfaces. VLANs with Layer 3 interfaces must also participate in Split MultiLink Trunking (SMLT).

syntax

`ip rsmlt`

Variable definitions

Use the data in the following table to help you use **`ip rsmlt`** command.

Variable	Value
`holddown-timer <0-3600>`	Defines how long the RSMLT switch does not participate in L3 forwarding. 0-3600 is the timer value in seconds. Avaya recommends that you configure this value to be longer than the anticipated routing protocol convergence.

Variable	Value
holdup-timer <0-9999>	The HoldUpTimer defines how long the RSMLT switch maintains forwarding for its peer. 0-9999 is the timer value in seconds. The value is a range from 0 to 3600 seconds or 9999. The value 9999 means infinity.
<cr>	Enables RSMLT. The no form of this command is **no ip rsmlt**.

Command mode

VLAN interface mode

default ip rsmlt

Use this command to return RSMLT to the default values on a VLAN.

syntax

default ip rsmlt

Command mode

VLAN interface mode

no ip rsmlt

Use this command to disable RSMLT on a VLAN to the default values on a VLAN.

syntax

no ip rsmlt

Command mode

VLAN interface mode

mlt members

Use this command to add members to the MultiLink Trunking (MLT) on the switch.

Syntax

mlt <*mid*> **member** <*slot/ports*>

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **mlt** <*mid*> **member** <*slot/ports*> command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.
<*slots/ports*>	Specifies the applicable members in member list form: **{** *slot/port* **[-** *slot/port* **] [, ...]}**.

Command mode

Global configuration mode

mlt add-vlan

Use this command to add an existing VLAN to the MultiLink Trunking (MLT) on the switch.

Syntax

mlt <*mid*> **add-vlan** <*vid*>

Variable definitions

Use the following table to help you use the **mlt** <*mid*> **add-vlan** <*vid*> command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.
<*vid*>	Specifies the VLAN ID.The default range of values is 1 to 4000.

Command mode

Global configuration mode

mlt name

Use this command to name the MultiLink Trunk (MLT) on the switch.

Syntax

mlt <*mid*> **name** <*string*>

Variable definitions

Use the following table to help you use the **mlt** <*mid*> **name** <*string*> command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.
<*string*>	Specifies the name of the MLT. The range of values is 0 to 20 alphanumeric characters.

Command mode

Global configuration mode

no mlt members

Use this command to remove members from the MultiLink Trunking (MLT) on the switch.

Syntax

no mlt <*mid*> **member** <*slot/ports*>

Variable definitions

Use the following table to help you use the **no mlt** <*mid*> **member** <*slot/ports*> command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.
<*ports*>	Specifies the applicable members in member list form: **{** *slot/port* **[-** *slot/port* **]** **[, ...]}**.

Command mode

Global configuration mode

mlt remove-vlan

Use this command to remove a VLAN from the MultiLink Trunking (MLT) on the switch.

Syntax

mlt <*mid*> **remove-vlan** <*vid*>

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **mlt** <*mid*> **remove-vlan** <*vid*> command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 4000.

Command mode

Global configuration mode

mlt create

Use this command to create the specified MultiLink Trunking (MLT) on the switch.

Syntax

mlt <*mid*> **create**

Variable definitions

Use the following table to help you use the **mlt** <*mid*> **create** command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

mlt encapsulation

Use this command to set tagging for the specified MultiLink Trunking (MLT) on the switch.

Syntax

mlt <*mid*> **encapsulation dot1q**

Variable definitions

Use the following table to help you use the **mlt** <*mid*> **encapsulation dot1q** command.

Variable	Value
<*mid*>	specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

no mlt encapsulation

Use this command to removes tagging for the specified MultiLink Trunking (MLT) on the switch.

Syntax

no mlt <*mid*> **encapsulation dot1q**

Variable definitions

Use the following table to help you use the **no mlt** <*mid*> **encapsulation dot1q** command.

Variable	Value
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

no mlt

Use this command to delete the specified MultiLink Trunking (MLT) on the switch.

Syntax

no mlt <*mid*>

Variable definitions

Use the following table to help you use the **no mlt** <*mid*> command.

Variable	Value
<*mid*>	specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

spanning-tree stp

Use this command to set general Spanning Tree environment variables.

Syntax

`spanning-tree stp` <*sid*> **`[forward-delay`** <*timeval*> **`] [group-stp <enable|disable> ] [hello-interval`** <*timeval*> **`] [max-age`** <*timeval*> **`] [priority`** <*number*> **`] [trap-stp <enable|disable> ]`**

Variable definitions

Use the following table to help you use the **`spanning-tree stp`** <*sid*> **`[forward-delay`** <*timeval*> **`] [group-stp <enable|disable> ] [hello-interval`** <*timeval*> **`] [max-age`** <*timeval*> **`] [priority`** <*number*> **`] [trap-stp <enable|disable> ]`** command.

Variable	Value
<*sid*>	Specifies the STG ID. The range of values is 1 to 64.
[forward-delay <*timeval*>]	Specifies the bridge forward delay time in 1/100 seconds. The range of values is 400 to 3000. The default is 1500 (15 seconds).
[group-stp <enable|disable>]	Enables or disables the spanning tree protocol on the specified STG. The default is enable.
[hello-interval <*timeval*>]	Specifies the bridge hello time in 1/100 seconds. The range of values is 100 to 1000. The default is 200 (2 seconds).
[max-age <*timeval*>]	Specifies the bridge maximum age time in 1/100 seconds. The range of values is 600 to 4000. The default is 2000 (20 seconds).
[priority <*number*>]	Specifies the bridge priority number of the specified port. The range of values is 0 to 65535. The default is 32768.
[trap-stp <enable|disable>]	Enables or disables the spanning tree protocol trap for the specified STG. The default is enable.

Command mode

Global configuration mode

spanning-tree stp add-ports

Use this command to add ports to a Spanning Tree Group (STG).

Syntax

`spanning-tree stp` <*sid*> **`add-ports`** <*value*>

Variable definitions

Use the following table to help you use the **`spanning-tree stp`** <*sid*> **`add-ports`** <*value*> command.

Variable	Value
<*sid*>	Specifies the STG ID. The range of values is 1 to 64.
<*value*>	Specifies the applicable ports in port list form: *{ slot/port [- slot/port][, ...]}*.

Command mode

Global configuration mode

spanning-tree stp create

Use this command to create a new Spanning Tree Group (STG).

Syntax

`spanning-tree stp` <*sid*> **`create [`** <*ports*> **`] [vlan`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`spanning-tree stp`** <*sid*> **`create [`** <*ports*> **`] [vlan`** <*value*> **`]`** command.

Variable	Value
<*sid*>	Specifies the STG ID. The range of values is 1 to 64.
[<ports>]	Specifies the applicable ports in port list form: *{ slot/port [- slot/port][, ...]}*.
`[vlan` <*value*> **`]`**	Specifies the VLAN ID.

Comments? infodev@avaya.com

Variable	Value
	Important: If a VLAN spans multiple switches, it must be within the same STG across all switches.

Command mode

Global configuration mode

spanning-tree stp remove-ports

Use this command to remove ports from a Spanning Tree Group (STG).

Syntax

`spanning-tree stp` <*sid*> **`remove-ports`** <*value*>

Variable definitions

Use the following table to help you use the **`spanning-tree stp`** <*sid*> **`remove-ports`** <*value*> command.

Variable	Value
<*sid*>	Specifies the Spanning Tree group ID. The range of values is 1 to 64.
<*value*>	Specifies the applicable ports in port list form: *{ slot/port [- slot/port][, ...]}*.

Command mode

Global configuration mode

no spanning-tree

Use this command to delete the specified Spanning Tree Group (STG).

Syntax

`no spanning-tree` <*sid*>

Variable definitions

Use the following table to help you use the **`no spanning-tree`** <*sid*> command.

Variable	Value
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64.

Command mode

Global configuration mode

telnet-access

Use this command to define parameters for the telnet login environment.

Syntax

`telnet-access <login-timeout> <sessions>`

Variable definitions

Use the following table to help you use the **`telnet-access <login-timeout> <sessions>`** command.

Variable	Value
`login-timeout`	Specifies the login timeout. The range is 30 to 65535. The default is 900 seconds.
`sessions`	Specifies number of sessions. The range is 0 to 8. The default is 8.

Command mode

Global configuration mode

vlan action

Use this command to flush dynamically learned entries from a table.

Syntax

`vlan action` <*vid*> **`<none | flush | MacFdb | flushArp | flushIp | all >`**

Variable definitions

Use the following table to help you use the **`vlan action`** <*vid*> **`<none | flush | MacFdb | flushArp | flushIp | all >`** command.

Comments? infodev@avaya.com

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
`none`	Specifies no table is flushed.
`flush MacFdb`	Specifies flushing of MacFdb table.
`flushArp`	Specifies flushing of Arp table.
`flushIp`	Specifies flushing of the IP table.
`all`	Specifies flushing of all tables.

Command mode

Global configuration mode

vlan add-mlt

Use this command to add MultiLink Trunking (MLT) to a Virtual LAN (VLAN).

Syntax

`vlan add-mlt` <*vid*> **`<mid>`**

Variable definitions

Use the following table to help you use the **`vlan add-mlt`** <*vid*> **`<mid>`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mid*>	Specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

vlan members

Use this command to add one or more ports to an existing Virtual LAN (VLAN).

Syntax

`vlan members <add|remove>` <*vid*> <*ports*> *[<member value>]*

Variable definitions

Use the following table to help you use the **`vlan members <add|remove>`** *<vid> <ports> [<member value>]* command.

Variable	Value
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<ports>	Specifies the applicable ports in port list form *{ slot/port [- slot/port][, ...]}*
[<member value>]	Specifies the port member type. The options are: • portmember (always a member), • static (always a member), or • notallowed (never a member).
<add | remove>	Add or remove a port from the VLAN.

Command mode

Global configuration mode

vlan name

Use this command to change the name of a Virtual LAN (VLAN).

Syntax

`vlan name` *<vid> <vname>*

Variable definitions

Use the following table to help you use the **`vlan name`** *<vid> <vname>* command.

Variable	Value
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<vname>	Specifies the VLAN name. The range of values is a string of 0 to 20 characters. The default VLAN name is VLAN <vid>.

Command mode

Global configuration mode

vlan qos-level

Use this command to set a Quality of Service (QoS) level for the specified Virtual LAN (VLAN).

Syntax

`vlan qos-level` <*vid*> <*integer*>

Variable definitions

Use the following table to help you use the **`vlan qos-level`** <*vid*> <*integer*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*integer*>	Specifies the QoS level. The range of values is 0 to 7. Level 7 is reserved and cannot be set.

Command mode

Global configuration mode

no vlan

Use this command to delete a Virtual LAN (VLAN).

Syntax

`no vlan` <*vid*>

Variable definitions

Use the following table to help you use the **`no vlan <vid>`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

vlan create type port

Use this command to create a port-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type port** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type port** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters. The default name is VLAN <vid>.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ApltkEther2Snap

Use this command to create an ApltkEther2Snap protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-ApltkEther2Snap** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-ApltkEther2Snap** <*sid*> **[color** <*value*> **]** command.

Comments? infodev@avaya.com

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-decEther2

Use this command to create a decEther2 protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-decEther2`** <*sid*> **`[color`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-decEther2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-decOtherEther2

Use this command to create a decOtherEther2 protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-decOtherEther2** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-decOtherEther2** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipEther2

Use this command to create an ipEther2 protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-ipEther2** <*sid*> **[color** <*value*> **]**

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-ipEther2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipv6Ether2

Use this command to create an ipv6Ether2 protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-ipv6Ether2`** <*sid*> **`[color`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-ipv6Ether2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.

Variable	Value
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipx802.2

Use this command to create an ipx802.2 protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-ipx802.2`** <*sid*> **`[color`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-ipx802.2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

Comments? infodev@avaya.com

vlan create type protocol-ipx802.3

Use this command to create an ipx802.3 protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-ipx802.3** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-ipx802.3** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipxEther2

Use this command to create an ipxEther2 protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-ipxEther2** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-ipxEther2** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipxSnap

Use this command to create an ipxSnap protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-ipxSnap`** <*sid*> **`[color`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-ipxSnap`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-Netbios

Use this command to create a Netbios protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-Netbios** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-Netbios** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-RarpEther2

Use this command to create a RarpEther2 protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-RarpEther2** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-RarpEther2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN.The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-sna802.2

Use this command to create a sna802.2 protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-sna802.2`** <*sid*> **`[color`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-sna802.2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.

Comments? infodev@avaya.com

Variable	Value
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-snaEther2

Use this command to create a snaEther2 protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-snaEther2`** <*sid*> **`[color`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-snaEther2`** <*sid*> **`[color`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN.The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-Userdef

Use this command to create a Userdef protocol-based Virtual LAN (VLAN).

Syntax

`vlan create` <*vid*> **`[name`** <*value*> **`] type protocol-Userdef`** <*sid*> <*pid*> **`[color`** <*value*> **`] [encap`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`vlan create`** <*vid*> **`[name`** <*value*> **`] type protocol-Userdef`** <*sid*> <*pid*> **`[color`** <*value*> **`] [encap`** <*value*> **`]`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
<*pid*>	Specifies a user-defined protocol not included in the list.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).
[encap <*value*>]	Specifies the frame encapsulation method.The values are ethernet-ii, llc,and snap. The default is all encapsulation types.

Command mode

Global configuration mode

vlan create type protocol-vinesEther2

Use this command to create a vinesEther2 protocol-based Virtual LAN (VLAN).

Comments? infodev@avaya.com

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-vinesEther2** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-vinesEther2** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-xnsEther2

Use this command to create a xnsEther2 protocol-based Virtual LAN (VLAN).

Syntax

vlan create <*vid*> **[name** <*value*> **] type protocol-xnsEther2** <*sid*> **[color** <*value*> **]**

Variable definitions

Use the following table to help you use the **vlan create** <*vid*> **[name** <*value*> **] type protocol-xnsEther2** <*sid*> **[color** <*value*> **]** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <*value*>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.

Variable	Value
<*sid*>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <*value*>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan fdb-entry aging-time

Use this command to set the forwarding database aging timer for a Virtual LAN (VLAN).

Syntax

`vlan fdb-entry` <*vid*> **`aging-time`** <*seconds*>

Variable definitions

Use the following table to help you use the **`vlan fdb-entry`** <*vid*> **`aging-time`** <*seconds*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*seconds*>	Specifies the timeout period in seconds. The range of values is 10 to 1000000. The default is 300.

Command mode

Global configuration mode

vlan fdb-entry flush

Use this command to flush the forwarding database for a Virtual LAN (VLAN).

Syntax

`vlan fdb-entry` <*vid*> **`flush`**

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`vlan fdb-entry`** <*vid*> **`flush`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Global configuration mode

vlan fdb-entry qos-level

Use this command to specify the parameters for the forwarding database and set the QoS Level of a Virtual LAN (VLAN). To set the QoS level, the entry must be in the forwarding database (FDB).

Syntax

`vlan fdb-entry` <*vid*> **`qos-level`** <*mac*> <*0...7*>

Variable definitions

Use the following table to help you use the **`vlan fdb-entry`** <*vid*> **`qos-level`** <*mac*> <*0...7*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mac*>	Specifies the MAC address.
<*0...7*>	Specifies the QoS level. The range of values is 0 to 7. Level 7 is reserved and cannot be set.

Command mode

Global configuration mode

vlan fdb-entry sync

Use this command to synchronize the forwarding database of the switch with the forwarding database of the other aggregation switch.

Syntax

`vlan fdb-entry` <*vid*> **`sync`**

Variable definitions

Use the following table to help you use the **`vlan fdb-entry`** <*vid*> **`sync`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

vlan fdb-filter add

Use this command to create a filter that can be applied to an entry in the Forwarding Database (FDB).

Syntax

`vlan fdb-filter` <*vid*> **`add`** <*mac*> <*port value*> **`drop <none|srcOnly|dstonly|Both> qos <level>`**

Variable definitions

Use the following table to help you use the **`vlan fdb-filter`** <*vid*> **`add`** <*mac*> <*port value*> **`drop <none|srcOnly|dstonly|Both> qos <level>`** command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mac*>	Specifies the MAC address.
<*port value*>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
action	none srcOnly dstOnly Both

Command mode

Global configuration mode

Comments? infodev@avaya.com

no vlan fdb-filter

Use this command to remove Virtual LAN (VLAN) filter members.

Syntax

no vlan fdb-filter <*vid*> <*mac*>

Variable definitions

Use the following table to help you use the **no vlan fdb-filter** <*vid*> <*mac*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mac*>	Specifies the MAC address.

Command mode

Global configuration mode

vlan fdb-static add

Use this command to add a static member to a Virtual LAN (VLAN) bridge.

Syntax

vlan fdb-static <*vid*> **add** <*mac*> <*port value*> **[** <*qos value*> **]**

Variable definitions

This command includes the following parameters:

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mac*>	Specifies the multicast MAC address.
<*port value*>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
Operational parameter: [<*qos value*>]	Specifies the Quality of Service level. The QoS level range is 0 to 7. Level 7 is reserved. The default is 1.

Command mode

Global configuration mode

no vlan fdb-static

Use this command to remove Virtual LAN (VLAN) static members.

Syntax

no vlan fdb-static <*vid*> <*mac*>

Variable definitions

Use the following table to help you use the **no vlan fdb-static** <*vid*> <*mac*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mac*>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac add

Use this command to add static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

vlan static-mcastmac <*vid*> **add** <*mac*> **[mlt <mid>] [ports** <*ports*>*]*

Variable definitions

Use the following table to help you use the **vlan static-mcastmac** <*vid*> **add** <*mac*> **[mlt <mid>] [ports** <*ports*>*]* command.

Variable	Value
<*mac*>	Specifies the MAC address.
[mlt <mid>]	Specifies the MultiLink Trunking ID. The range is 1 to 31.
[ports <*ports*>]	Specifies the port(s) to receive the multicast flooding.

Command mode

Global configuration mode

For more information about configuring VLAN, see *Configuring IP Multicast Routing Protocols*.

vlan static-mcastmac add-mlt

Use this command to add MultiLink Trunking (MLT) to static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

`vlan static-mcastmac` <*vid*> **`add-mlt`** <*mid*>

Variable definitions

Use the following table to help you use the **`vlan static-mcastmac`** <*vid*> **`add-mlt`** <*mid*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
`<mid>`	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<*mac*>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac remove-mlt

Use this command to delete MultiLink Trunking (MLT) to static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

`vlan static-mcastmac` <*vid*> **`remove-mlt ports <ports/slots>`** <*mac*>

Variable definitions

Use the following table to help you use the **`vlan static-mcastmac`** <*vid*> **`remove-mlt ports <ports/slots>`** <*mac*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<*mid*>	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<*mac*>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac add-ports

Use this command to add ports to static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

`vlan static-mcastmac` <*vid*> **`add-ports`** <*ports*> <*mac*>

Variable definitions

Use the following table to help you use the **`vlan static-mcastmac`** <*vid*> **`add-ports`** <*ports*> <*mac*> command.

Variable	Value
<*ports*>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][,...]}*.
<*mac*>	Specifies the MAC address.
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

vlan static-mcastmac remove

Use this command to remove MAC-to-VLAN static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

`vlan static-mcastmac` <*vid*> **`remove <mid>`** <*mac*>

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`vlan static-mcastmac`** <*vid*> **`remove <mid>`** <*mac*> command.

Variable	Value
<*mid*>	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<*mac*>	Specifies the MAC address.
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

For more information about configuring VLAN, see *Configuring IP Multicast Routing Protocols*.

vlan static-mcastmac remove-mlt

Use this command to remove MultiLink Trunking (MLT) from static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

`vlan static-mcastmac` <*vid*> **`remove-mlt <mid>`** <*mac*>

Variable definitions

Use the following table to help you use the **`vlan static-mcastmac`** <*vid*> **`remove-mlt <mid>`** <*mac*> command.

Variable	Value
<*mid*>	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

vlan static-mcastmac remove-ports

Use this command to delete ports from the Layer 2 multicast Media Access Control (MAC) entries on a Virtual LAN (VLAN).

Syntax

no vlan static-mcastmac <*vid*> **remove-ports <mid>** <*mac*>

Variable definitions

Use the following table to help you use the **no vlan static-mcastmac** <*vid*> **remove-ports <mid>** <*mac*> command.

Variable	Value
<mid>	Specifies the MultiLink Trunking ID.
<*mac*>	Specifies the MAC address.
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

no vlan static-mcastmac

Use this command to delete Layer 2 multicast Media Access Control (MAC) entries on a Virtual LAN (VLAN).

Syntax

no vlan static-mcastmac <*vid*> **mac** <*mac*>

Variable definitions

Use the following table to help you use the **no vlan static-mcastmac** <*vid*> **mac** <*mac*> command.

Variable	Value
<*mac*>	Specifies the MAC address.
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

interface vlan

Use this command to interface with a Virtual LAN (VLAN).

Syntax

`interface vlan` <*vid*>

Variable definitions

Use the following table to help you use the **`interface vlan`** <*vid*> command.

Variable	Value
<*vid*>	Specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

ip address

Use this command to assign an IP address and subnet mask to a Virtual LAN (VLAN).

Syntax

`ip address` <*ipaddr mask*>

Variable definitions

Use the following table to help you use the **`ip address`** <*ipaddr mask*> command.

Variable	Value
<*ipaddr*>	Specifies the IP address.
<*mask*>	Specifies the subnet mask **`{a.b.c.d}`**.

Command mode

Interface configuration mode

ip vrf

Use this command to create and configure a VRF instance to provide a virtual routing interface for a user.

Syntax

ip vrf <WORD 0-32>

<WORD 0-32> is the name of the VRF instance with a string length of 0 to 32.

Variable definitions

Use the data in the following table to help you use the **ip vrf <WORD 0-32>** command.

Variable	Value
<cr>	Creates the VRF instance with the name specified.
max-routes <0-8000>	Specifies the maximum number of routes for the VRF.
max-routes-trap enable	Enables the sending of traps after the maximum number of routes is reached.
name <WORD 0-32>	Renames the VRF instance.
vrf-trap enable	Enables the switch to send VRF-related traps.
vrfids <1-127>	Specifies the VRF ID.

Command mode

Global configuration mode

vrf

Use this command to associate a VLAN with a VRF.

Syntax

vrf <WORD 0-32>

<WORD 0-32> is the name of the VRF instance with a string length of 0 to 32.

Command mode

VLAN Interface configuration mode

Comments? infodev@avaya.com

Chapter 11: Route filters commands

This chapter describes ACLI route filters commands and their parameters.

Navigation

- filter acl ip on page 308
- filter acl non-ip on page 308
- filter acl action on page 309
- filter acl ace on page 311
- no filter acl ace on page 312
- no filter acl on page 313
- show filter acl advanced on page 313
- filter acl ethernet on page 314
- filter acl ip-hdr on page 315
- filter acl port on page 317
- filter acl protocol on page 318
- filter acl debug on page 319
- filter acg on page 320
- filter acg modify on page 320
- no filter acg on page 321
- filter act ethernet on page 321
- filter act ip-hdr on page 323
- no filter act on page 326
- filter act on page 326
- filter act pattern on page 327
- no filter act pattern on page 328
- show filter act on page 328

filter acl ip

Use this command to create a new IP ACL.

Syntax

`filter acl` <*acl-id*> **`ip [acl-name`** <*value*> **`] [act-id`** <*value*> **`]`**

Important:

ACLs can be of either type. Access Control Entities (ACEs) can match packets classified as 'ip' (ip header and below) or 'non-ip' (ethernet header).

Variable definitions

Use the following table to help you use the **`filter acl`** <*acl-id*> **`ip [acl-name`** <*value*> **`] [act-id`** <*value*> **`]`** command.

Variable	Value
acl-name <*value*>	A descriptive name that identifies this ACL. The value is a unique identifier (from 1 to 512) for this ACL entry. If you do not assign a name, the system automatically assigns one.
act-id	Identifies the access control template (ACT) bound to this interface. act-id - the range is 1 to 2. If you do not assign a ACT, the system automatically uses act-id 1 **Important:** The rules in the ACL specified in AclIdList must be a subset of the values defined in the ACT entry.

Command mode

Global configuration mode

filter acl non-ip

Use this command to create a new non-IP ACL.

Syntax

```
filter acl <acl-id> non-ip <acl-name> <act-id>
```


Comments? infodev@avaya.com

Important:

ACLs can be of either type. Access Control Entities (ACEs) can match packets classified as 'ip' (ip header and below) or 'non-ip' (ethernet header).

Variable definitions

Use the following table to help you use the **`filter acl <acl-id> non-ip <acl-name> <act-id>`** command.

Variable	Value
<acl-id>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<act-id>	Specifies the ACT ID (from 1 to 2) for this ACL entry.

Command mode

Global configuration mode

filter acl action

Use this command to create and configure an ACE.

Syntax

```
filter acl <acl-id> action <ace-id> <mode> [trust-dscp <value>]
[remark-dscp <value>] [remark-user-priority <value>] [police <value>
<ace-name>] [precedence <value>] [traffic-type <value>]
```

Variable definitions

Use the following table to help you use the **`filter acl <acl-id> action <ace-id> <mode> [trust-dscp <value>] [remark-dscp <value>] [remark-user-priority <value>] [police <value> <ace-name>] [precedence <value>] [traffic-type <value>]`**command.

Variable	Value
<acl-id>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<act-id>	Specifies the ACT ID (from 1 to 2) for this ACL entry.
<mode>	Specifies the operating mode associated with this ACE. Enter one of the following modes to determine what action the ACE takes when it matches a packet:

Variable	Value
	• inactive—no affect on traffic • permit—permits traffic • deny—denies traffic • redirect—redirects traffic • fwd2cpu—forwards to the central processing unit (CPU
next-hop <*ipaddr*>	<*next-hop*> is an IP address {a.b.c.d}. This value redirects matching IP traffic to the next hop, as specified by this IP address.
trust-dscp <*enable*|*disable*>	Specifies trust dscp.
remark-dscp <*value*>	Causes DSCP to re-mark non-standard traffic classes so it uses a local per hop behavior (PHB). The range is 0 to 63. <*value*> is one of the following choices: disable phbcs0 phbcs1 phbaf11 phbaf12 phbaf13 phbcs2 phbaf21 phbaf22 phbaf23 phbcs3 phbaf31 phbaf32 phbaf33 phbcs4 phbaf41 phbaf42 phbaf43 phbcs5 phbef phbcs6 phbcs7 The default setting is disable.
remark-user-priority <*value*>	Sets the User Priority as described by Layer 2 standards: 802.1Q, 802.1p. value is one of the following choices: • ignore | zero | one | ... | seven • 0 ... 7 The default setting is ignore.
police <*value*>	police <*value*> sets the desired policing profile identifier in the range from 0 to 128. When policing is not desired, set to disable (0).
<*ace-name*>	<*ace-name*> is a string that names the ACE. The range is 0 to 255. If you do not assign a name, the system automatically assigns one.
next-hop <*ipaddr*>	<*next-hop*> is an IP address {a.b.c.d}. This value redirects matching IP traffic to the next hop, as specified by this IP address.
precedence <*0 to 255*>	*precedence* sets the order for when each ACE is applied within an ACL. This value is

Comments? infodev@avaya.com

Variable	Value
	in the range from 0 to 255, and the default is 0. An ACL can contain multiple ACEs that match a packet. The lower the value that you assign to an ACE increases its order of precedence. For example, the highest precedence that you can assign to an ACE is 0, and the lowest precedence (256) is reserved for the default ACE.
traffic-type <*value*>	<*traffic-type*> <value> can be: {all | bridged | routed | tagged | tagged-bridged | tagged-routed | untagged | untagged-bridged | untagged-routed}. • **`all`** - matches both bridged and routed packets. • **`bridged`** - matches bridged packets. • **`routed`** - matches IPv4 unicast routed packets. • tagged • untagged • tagged-bridged • tagged-routed • untagged-bridged • untagged-routed The default setting is **`all`**. This value indicates the type of packets that the ACE is set to match.

Command mode

Global configuration mode

filter acl ace

Use this command to create an advanced ACE entry

Syntax

```
filter acl ace advanced <acl-id> <ace-id> <pattern-id> <operator>
```

Variable definitions

Use the following table to help you use the **`filter acl ace advanced <acl-id> <ace-id> <pattern-id> <operator>`** command.

Variable	Value
<acl-id>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<ace-id>	Specifies the unique identifier (from 1 to 256) for this ACE entry.
<operator>	Specifies the ACE operator. Values include the following: • any—the default pattern field match condition operator • eq—the equals-to pattern field match condition operator • ne—the not equals-to pattern field match condition operator • le—the less-than pattern field match condition operator • ge—the greater-than pattern field match condition operator • range—sets a pattern field match condition operator range • mask—the pattern field match condition operator mask
<pattern-id>	Identifies the filter pattern. Values range from 1 to 40.

Command mode

Global configuration mode

no filter acl ace

Use this command to delete an advanced ACE entry

Syntax

```
no filter acl ace advanced <acl-id> <ace-id> <pattern-id>
```


Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`filter acl ace advanced <acl-id> <ace-id> <pattern-id>`** command.

Variable	Value
<*acl-id*>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<*ace-id*>	Specifies the unique identifier (from 1 to 256) for this ACE entry.
<*pattern-id*>	Identifies the filter pattern. Values range from 1 to 40.

Command mode

Global configuration mode

no filter acl

Use this command to delete an ACL or an ACE.

Syntax

`no filter acl <acl-id> [<ace-id>]`

Variable definitions

Use the following table to help you use the **`no filter acl <acl-id> [<ace-id>]`** command.

Variable	Value
<*acl-id*>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<*ace-id*>	Specifies the unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

show filter acl advanced

Use this command to view filter pattern and ACT matching information.

Syntax

`show filter acl advanced`

Command mode

Global configuration mode

Variable definitions

The following table describes optional parameters that you enter after the **`show filter acl advanced`** command.

Variable	Value
`<ace-id>`	Identifies the ACE. Values range from 1 to 512.
`<acl-id>`	Identifies the ACL. Values range from 1 to 256.

filter acl ethernet

Use this command to configure an ACE's Ethernet values.

Syntax

`filter acl <acl-id> ethernet <ace-id> src-mac <value> <ace-op> <src-mac> dst-mac <value> <ace-op> <dst-mac> ether-type <value> vlan-id <value> user-priority <value>`

Variable definitions

Use the following table to help you use the **`no filter acl <acl-id> [<ace-id>]`** command.

Variable	Value
<*acl-id*>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<*ace-id*>	Specifies the unique identifier (from 1 to 256) for this ACE entry.
src-mac <*value*> <*ace-op*> <*src-mac*>	Specifies the MAC source address to match {a:b:c:d}. <*ace-op*> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <*src-mac*> sets the mask or higher address for MAC source address, when ace-op is set to mask or range.

Comments? infodev@avaya.com

Variable	Value
dst-mac <*value*> <*ace-op*> <*dst-mac*>	Specifies the MAC source address to match {a:b:c:d:e:f}. <*ace-op*> specifies the logical operator: {any | eq | ne | le | ge | range | mask}. The default is any. <*dst-mac*> sets the mask or higher address for MAC destination address, when ace-op is set to mask or range.
ether-type <*value*>	Specifies the EtherType value from the Ethernet header. • ip • arp • rarp • appleTalk • decLat • ipv6 • any (outside valid range) The default is any.
vlan-id <*value*>	Specifies the Vlan-ID to match. This value is in the range of 1 - 2000. If the flag vid-max4k is set the range is 1 to 4000. The default is 0.
user-priority <*value*>	Sets the Priority bits (3-bit value) from the 802.1Q/p. <*value*> is one of the following choices: • 0...7 • 0x0...0x07 • ignore|zero|one|two|three|four|five|six|seven The default setting is ignore.

Command mode

Global configuration mode

filter acl ip-hdr

Use this command to configure an ACE's IP values.

Syntax

```
filter acl <acl-id> ip <ace-id> [src-ip <value> <ace-op> <src-ip>]
[dst-ip <value> <ace-op> <dst-ip>] [dscp <value> <ace-op> <dscp>]
ipfragment <value>
```

Variable definitions

Use the following table to help you use the **`filter acl <acl-id> ip <ace-id> [src-ip <value> <ace-op> <src-ip>] [dst-ip <value> <ace-op> <dst-ip>] [dscp <value> <ace-op> <dscp>] ipfragment <value>`** command.

Variable	Value
<*ace-id*>	Specifies a unique identifier (from 1 to 256) for this ACE entry.
<*acl-id*>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
src-ip <*value*> <*ace-op*> <*src-ip*>	Specifies the IP source address to match *{a.b.c.d}* from the IP header. <*ace-op*> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <*src-ip*> sets the mask or higher address for the IP source address, when: *ace-op* is set to mask or range.
dst-ip <*value*> <*ace-op*> <*dst-ip*>	Specifies the IP destination address to match from the IP header. <*ace-op*> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <*dst-ip*> sets the mask or higher address for the IP destination address, when: *ace-op* is set to mask or range.
dscp <*value*> <*ace-op*> <*dscp*>	Causes DSCP to re-mark non-standard traffic classes so it uses a local per hop behavior (PHB). <*value*> is one of the following choices: disable phbcs0 phbcs1 phbaf11 phbaf12 phbaf13 phbcs2 phbaf21 phbaf22 phbaf23 phbcs3 phbaf31 phbaf32 phbaf33 phbcs4 phbaf41 phbaf42 phbaf43 phbcs5 phbef phbcs6 phbcs7 The default setting is disable. <*ace-op*> specifies the logical operator: any | eq | ne | le | ge | range | mask The default is any.

Comments? infodev@avaya.com

Variable	Value
	<*dscp*> sets the mask or higher address for the DSCP value, when: *ace-op* is set to mask or range.
pfragment<*value*>	Set the match option for IP fragmented packets. The value is one of the following: • any = any packet • fragments = IP fragemented packets only • non-fragments = non-IP fragmented packets only The default is any. **Important:** This option must be set whenever a match on an L4 field is required. This field will be automatically set to either 'non-fragments' or 'any' whenever an L4 field is set or unset.

Command mode

Global configuration mode

filter acl port

Use this command to configure an ACE's port values.

Syntax

`filter acl` <*acl-id*> **`port`** <*ace-id*> **`src-port`** <*value*> <*ace-op*> <*src-port*> **`dst-port`** <*value*> <*ace-op*> <*dst-port*>

Variable definitions

Use the following table to help you use the **`filter acl`** <*acl-id*> **`port`** <*ace-id*> **`src-port`** <*value*> <*ace-op*> <*src-port*> **`dst-port`** <*value*> <*ace-op*> <*dst-port*> command.

Variable	Value
<*ace-id*>	Specifies a unique identifier (from 1 to 256) for this ACE entry.
<*acl-id*>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
src-port <*value*> <*ace-op*> <*src-port*>	Specifies the TCP or UDP source port to match.<*value*> is one of the following choices:

Variable	Value
	• 0...65535 • 0x0...0xffff <*ace-op*> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <*src-port*> sets the TCP or UDP source port, when: *ace-op* is set to mask or range.
dst-port <*value*> <*ace-op*> <*dst-port*>	Specifies the TCP or UDP destination port to match. <*value*> is one of the following choices: • 0...65535 • 0x0...0xffff • any|bgp|bootpstrap|bootpd-dhcp|dns|echo|ftpcontrol|ftpdata|hdot323|http|rip|rtp|rtcp|ssh|telnet|tftp <*ace-op*> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <*dst-port*> sets the mask or higher address for the TCP or UDP destination port, when: *ace-op* is set to mask or range.

Command mode

Global configuration mode

filter acl protocol

Use this command to configure an ACE's protocol values.

Syntax

`filter acl` <*acl-id*> **`protocol`** <*ace-id*> <*ip-protocol*> <*ace-op*> <*ip-protocol*>

Variable definitions

Use the following table to help you use the **`filter acl`** <*acl-id*> **`protocol`** <*ace-id*> <*ip-protocol*> <*ace-op*> <*ip-protocol*> command.

Variable	Value
<*ace-id*>	Specifies a unique identifier (from 1 to 256) for this ACE entry.

Comments? infodev@avaya.com

Variable	Value
<acl-id>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<ace-op> <ip-protocol>	<ace-op> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <ip-protocol> sets the protocol, when: ace-op is set to mask or range.

Command mode

Global configuration mode

filter acl debug

Use this command to debug an ACE.

Syntax

```
filter acl <acl-id> debug <ace-id> match-count <value> mirror <value>
```

Variable definitions

Use the following table to help you use the **`filter acl <acl-id> debug <ace-id> match-count <value> mirror <value>`** command.

Variable	Value
<ace-id>	Specifies a unique identifier (from 1 to 256) for this ACE entry.
<acl-id>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
`match-count` *<value>*	Counts the packets and octets of matching traffic from all ports where the list is active. <value> is one of the following choices: • **`disable`** - Set this mode when counters are not required. This is the default. • **`bytes-pkts`** - Set this mode when the count of octets is accurately required. • **`kbytes-pkts`** - Set this mode when the octets count is desired in kilobytes. **Important:** There is potential for an overflow of the octet counter. For example, consider an interface with a forwarding rate of 17

Variable	Value
	million 64-byte pkts per second. If the statistics are accumulated from 10 such interfaces in a 64-bit counter, the counter could overflow in approximately a year.
mirror <*value*>	Mirrors matching packets. <value> is {enable | disable}. The default is disable.

Command mode

Global configuration mode

filter acg

Use this command to configure an Access Control Group (ACG), which may contain one each of ACL type ip and ACL type non-ip.

Syntax

```
filter acg <acg-id> <acl-id> <acg-name>
```

Variable definitions

Use the following table to help you use the **filter acg <acg-id> <acl-id> <acg-name>** command.

Variable	Value
<acl-id>	<acl-id> is a unique identifier (from 1 to 512) for this ACG entry.
<acg-name>	<acg-name> is a descriptive name that identifies this ACG. If you do not assign a name, the system automatically assigns one.

Command mode

Global configuration mode

filter acg modify

Use this command to modify an ACG's acl-id-list.

Syntax

```
filter acg <acg-id> modify <acl-id> <acg-name>
```


Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **filter acg <acg-id> modify <acl-id> <acg-name>** command.

Variable	Value
<acl-id>	Specifies a unique identifier (from 1 to 512) for this ACL entry.
<acg-name>	A descriptive name that identifies this ACG.
<acg-id>	Specifies a unique identifier (from 1 to 1024) for this ACG entry

Command mode

Global configuration mode

no filter acg

Use this command to delete an ACG.

Syntax

```
no filter acg <acg-id>
```

Variable definitions

Use the following table to help you use the **no filter acg <acg-id>** command.

Variable	Value
<acg-id>	Specifies a unique identifier (from 1 to 1024) for this ACG entry

Command mode

Global configuration mode

filter act ethernet

Use this command to create an Ethernet ACT.

Syntax

```
filter act <act-id> ethernet <acl-type> src-mask <value> dst-mask
<value> ether-type <value> vlan-mask <value> name <value>
```

Variable definitions

Use the following table to help you use the **`filter act <act-id> ethernet <acl-type> src-mask <value> dst-mask <value> ether-type <value> vlan-mask <value> name <value>`** command.

Variable	Value
act-id	Identifies the access control template (ACT) bound to this interface. The range is 1 to 2. **Important:** The rules in the ACL specified in AclIdList must be a subset of the values defined in the ACT entry. Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
src-mask <*value*>	Specifies a mask for the source MAC address. This mask is used by the ACEs that are members of the ACLs using this ACT. • A MAC address with all zeros indicates this value is not desired in the match criteria. • Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
dst-mask <*value*>	Specifies a mask for the destination MAC address. This mask is used by the ACEs that are members of the ACLs using this ACT. • A MAC address with all zeros indicates this value is not desired in the match criteria. • Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
ether-type <*value*>	Specifies a mask for the Ether type value to match. The range for this value is from 0 to 65535. • An Ether type of zero indicates this value is not desired in the match criteria. • Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
vlan-mask <*value*>	Specifies a mask for the VLAN tag information to match. This mask is for the first byte in 802.1Q/802.1p tagged frames that encode the VLAN ID in 12 bits. The range is 1 to 2.

Variable	Value
	• A value of zero indicates the VLAN Tag information is not desired in the match criteria. • Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
name <*value*>	A descriptive name that identifies this ACT. If you do not assign a name, the system automatically assigns one. The range is 0 to 255. **Important:** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.

Command mode

Global configuration mode

filter act ip-hdr

Use this command to configure an IP ACT.

Syntax

```
filter act <act-id> ip-hdr src-mask <value> dst-mask <value> protocol
<value> tos <value> src-port <value> dst-port <value> tcp-flags
<value> icmp <value>
```

Variable definitions

Use the following table to help you use the **`filter act <act-id> ip-hdr src-mask <value> dst-mask <value> protocol <value> tos <value> src-port <value> dst-port <value> tcp-flags <value> icmp <value>`** command.

Variable	Value
<*act-id*>	Specifies a unique identifier (from 1 to 2) for this ACT.
src-mask <value>	src-mask - <value> is one of the following: • 0.0.0.0 • 255.255.255.255 Specifies a mask for the source IP address.

Variable	Value
	• An IP address with all zeros indicates this value is not desired in the match criteria. • Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
dst-mask <value>	Specifies a mask for the destination IP address. dst-mask - <value> is one of the following: • 0.0.0.0 • 255.255.255.255 • A destination IP address with all zeros indicates this value is not desired in the match criteria. • Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
protocol <*value*>	Specifies a mask for the protocol value in the IP header to match. <value> can be one of: • 0...255 • 0x0...0xff. **Important:** A value of zero indicates this value is not desired in the match criteria.
tos <*value*>	Specifies a mask for the TOS byte (DSCP value) in the IP header to match. DSCP is encoded in the 6 most significant bits of the ToS byte (see RFC 2474). <value> can be one of: • 0...255 • 0x0...0xff. **Important:** A value of zero indicates this value is not desired in the match criteria.
src-port <*value*>	Specifies a mask for the source TCP/UDP port in TCP/UDP header to match. <value> can be one of: • 0...65535 • 0x0...0xffff.

Variable	Value
	Important: A value of zero indicates this value is not desired in the match criteria.
dst-port <*value*>	Specifies a mask for the destination TCP/UDP port in TCP/UDP header to match. <value> can be one of: • 0...65535 • 0x0...0xffff. **Important:** A value of zero indicates this value is not desired in the match criteria.
tcp-flags <*value*>	Specifies a mask for the 6 bits in the TCP flags value in the TCP header to match. <value> can be one of: • 0...63 • 0x0...0x3f. **Important:** A value of zero indicates this value is not desired in the match criteria.
icmp <*value*>	Specifies a mask for the ICMP message Type and Code to match. The 8-bit Type value is encoded in the MSB and the 8-bit Code value is encoded in the LSB. <value> can be one of: • 0...65535 • 0x0...0xffff. **Important:** A value of zero indicates this value is not desired in the match criteria.

Command mode

Global configuration mode

no filter act

Use this command to delete an ACT.

Syntax

no filter act <*act-id*> <*acl-type*>

Variable definitions

Use the following table to help you use the **no filter act** <*act-id*> <*acl-type*> command.

Variable	Value
<act-id>	Specifies a unique identifier (from 1 to 2) for the ACT entry.
<acl-type>	either ip or non-ip.

Command mode

Global configuration mode

filter act

Use this command to assign user-defined filter pattern templates.

Syntax

filter act *<act-id> advanced <acl-type> <pattern-id>*

Variable definitions

The following table describes variables that you enter in the**filter act** *<act-id> advanced <acl-type> <pattern-id>* command.

Variable	Value
<pattern-id>	Identifies the filter pattern. Values range from 1 to 40.
<act-id>	Identifies the ACT. Values range from 1 to 36.
<acl-type>	Specifies the type of ACL. Values are IP or non-IP.

Command mode

Global configuration mode

filter act pattern

Use this command to configure a filter pattern

Syntax

`filter act pattern` <*pattern-id*> <*base*> <*offset*> <*length*>

Variable definitions

The following table describes variables that you enter in the **`filter act pattern`** <*pattern-id*> <*base*> <*offset*> <*length*> command.

Variable	Value
`<pattern-id>`	Identifies the filter pattern. Values range from 1 to 40.
`<base>`	Specifies one of the following as the user-defined header for the ACEs of the ACL: • l2—starts at the beginning of the Ethernet frame • l2e—begins immediately following the Source Mac of the Ethernet frame for an untagged frame or immediately following the VLAN EtherType for a VLAN tagged frame • l3—begins immediately following the layer 2 encapsulation header • l4—begins at the header following the layer 3 header
`<length>`	Specifies the length, in bytes, of the filter pattern template. Valid values are from 1 to 16. For a base value of l2, the sum of the offset and length values must be less than 13. For a base value of l2e, the sum of the offset and length values must be less than 69. The length value ranges from 1 to 10. For a base value of l3 or l4, the sum of the offset and length values must be less than 67. The length value ranges from 1 to 16.
`<offset>`	Defines the user-defined field offset with the selected header option as a base. Valid values are from 0 to 67. For a base value of l2, the offset value must be in the range of 0 to 11.

Command mode

Global configuration mode

no filter act pattern

Use this command to delete a filter pattern

Syntax

no filter act pattern <*pattern-id*>

Command mode

Global configuration mode

show filter act

Use theis command to view filter pattern and ACT matching information.

Syntax

show filter act <1-36>

Command mode

Global configuration mode

Variable definitions

The following table describes optional parameters that you enter after the **show filter act <1-36>** command.

Variable	Value
<acl-id>	Identifies the ACT. Values range from 1 to 36.
<acl-type>	Specifies the type of ACL. Values are IP or non-IP.

Comments? infodev@avaya.com

Chapter 12: Test and diagnostic commands

This chapter describes ACLI test and diagnostic commands and their parameters.

Navigation

- clear port-stats on page 330
- clear telnet on page 330
- port-mirroring on page 331
- no port-mirroring on page 332
- rmon alarm on page 332
- no rmon alarm on page 333
- rmon event on page 334
- no rmon event on page 334
- rmon history on page 335
- no rmon history on page 336
- rmon memsize on page 336
- rmon stats on page 337
- no rmon stats on page 337
- rmon trap-option on page 338
- rmon util-method on page 338
- test on page 339
- trace auto-enable on page 339
- trace auto-enable add-module on page 340
- trace auto-enable auto-trace on page 341
- trace auto-enable remove-module on page 342
- trace clear on page 342
- trace filter on page 343
- trace grep on page 343
- trace level on page 343

- trace off on page 344
- trace route-policy on page 344
- trace screen on page 345
- traceroute on page 345
- vct test on page 346

clear port-stats

Use this command to clear port statistics from the switch counters.

Syntax

`clear port-stats [` *<portlist>* **`]`**

Variable definitions

Use the following table to help you use the **`clear port-stats [`** *<portlist>* **`]`** command.

Variable	Value
<portlist>	is an optional parameter that specifies the ports to be cleared in the port list form: *{slot/port[-slot/port][, ...]}*

Command mode

Privileged EXEC mode

clear telnet

Use this command to end a Telnet session.

Syntax

`clear telnet` *<session id>*

Variable definitions

Use the following table to help you use the **`clear telnet`** *<session id>* command.

Variable	Value
<session id>	Specifies the ID number of the Telnet session. The range of values is 0 to 7.

Command mode

Privileged EXEC mode

port-mirroring

Use this command to create a new entry in the port mirroring table for a specified port. Also use this command to specify the mirroring mode. You can configure up to 10 mirroring ports and one mirroring monitor port.

Important:

Avaya recommends that you delete port mirroring entries that are no longer needed to reduce the load on the switch.

Syntax

To create a NEW port mirroring entry, use the following syntax:

`mirror-by-port` <*id*> **`in-port`** <*slot/port*> **`out-port`** <*slot/port*> **`mode <tx|rx|both>`**

To enable the NEW port mirroring entry, use the following syntax:

`mirror-by-port` <*id*> **`enable`**

To modify an EXISTING port mirroring entry, use the following syntax:

`mirror-by-port` <*id*> **`mirror-port`** <*slot/port*> **`monitor-port`** <*slot/port*>

Variable definitions

Use the following table to help you use the **`mirror-by-port`** command.

Variable	Value
<*id*>	Specifies the port mirroring ID. The range is 1 to 383.
in-port <*slot/port*>	Specifies the slot and port to mirror for a new port mirroring table entry.
out-port <*slot/port*>	Specifies the slot and port to monitor for a new port mirroring table entry.
[mode] <tx|rx|both>	Specifies the mirroring port mode. • tx mirrors transmit packets. • rx mirrors receive packets. • both mirrors both transmit and receive packets.

Variable	Value
enable	Enables a mirroring port already created in the mirror-by-port table.
mirror-port <*slot/port*>	Specifies the mirroring port.
monitor-port <*slot/port*>	Specifies the mirrored port.

Command mode

Global configuration mode

no port-mirroring

Use this command to delete an entry in the port mirroring table.

Syntax

no mirror-by-port <*id*>

Variable definitions

Use the following table to help you use the **no mirror-by-port** command.

Variable	Value
<*id*>	Specifies the port mirroring ID. The range is 1 to 383.

Command mode

Global configuration mode

rmon alarm

Use this command to create an alarm interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

rmon alarm <*1-65535*> <*WORD*> <*1-3600*> **{absolute|delta} rising-threshold** <*-32768-65535*> **] falling-threshold** <*-32768-65535*> **] [owner** <*value*> **]**

Variable definitions

Use the following table to help you use the **rmon alarm** <*1-65535*> <*WORD*> <*1-3600*> **{absolute|delta} rising-threshold** <*-32768-65535*> **] falling-threshold** <*-32768-65535*> **] [owner** <*value*> **]** command.

Comments? infodev@avaya.com

Variable	Value
<*1-65535*>	Specifies the alarm interface index number. The range of values is 1 to 65535.
<*WORD*>	Specifies the alarm name. The name is case sensitive and its range of values is a string of 1 to 1536 characters.
<*1-3600*>	Specifies the sample interval. The range of values is 1 to 3600.
{absolute|delta}	Specifies the sample type. The options are: absolute and delta.
rising-threshold <-32768-65535>	Specifies the rising threshold. The range of values is *-32768* to *65535*.
<*1-65535*>	Specifies the rising event number.
falling-threshold <-32768-65535>	Specifies the falling threshold. The range of values is -32768 to 65535.
<*1-65535*>	Specifies the falling event number.
[owner <*value*>]	Specifies the name of the owner. The range of values is a string of 1 to 48 characters.

Command mode

Global configuration mode

no rmon alarm

Use this command to delete the specified Remote Monitoring (RMON) alarm.

Syntax

`no rmon alarm [` <*1-65535*> **`]`**

Variable definitions

Use the following table to help you use the **`no rmon alarm [`** <*1-65535*> **`]`** command.

Variable	Value
<*1-65535*>	Specifies an optional parameter that specifies the alarm index number. The range of values is 1 to 65535

Command mode

Global configuration mode

rmon event

Use this command to create a Remote Monitoring (RMON) event on the switch.

Syntax

rmon event <*1-65535*> **trap_src** <*value*> **trap_dest** <*value*> **[log-type** <*value*> **] [description** <*LINE*> **] [community** <*value*> **] [owner** <*LINE*> **]**

Variable definitions

Use the following table to help you use the **rmon event** <*1-65535*> **trap_src** <*value*> **trap_dest** <*value*> **[log-type** <*value*> **] [description** <*LINE*> **] [community** <*value*> **] [owner** <*LINE*> **]** command.

Variable	Value
<*1-65535*>	Specifies the event index number. The range of values is 1 to 65535.
trap_src <*value*>	Specifies the trap source IP address.
trap_dest <*value*>	Specifies the trap destination IP address.
[log-type <*value*>]	Specifies the event type. The options are: none, log, snmp-trap, or log-and-trap.
[description <*LINE*>]	Specifies the event description. The range of values is a string of 0 to 127 characters.
[community <*value*>]	Specifies the event community. The range of values is a string of 0 to 127 characters.
[owner <*LINE*>]	Specifies the owner. The range of values is a string of 1 to 48 characters.

Command mode

Global configuration mode

no rmon event

Use this command to delete the specified Remote Monitoring (RMON) event.

Syntax

no rmon event [<*1-65535*> **]**

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **no rmon event [** *<1-65535>* **]** command.

Variable	Value
<1-65535>	Specifies an optional parameter that specifies the event index number. The range of values is 1 to 65535.

Command mode

Global configuration mode

rmon history

Use this command to create a history control interface for Remote Monitoring (RMON) functions on the switch.

Syntax

rmon history *<1-65535>* *<ports>* **[buckets** *<value>* **] [intv** *<value>* **] [owner** *<LINE>* **]**

Variable definitions

Use the following table to help you use the **rmon history** *<1-65535>* *<ports>* **[buckets** *<value>* **] [intv** *<value>* **] [owner** *<LINE>* **]** command.

Variable	Value
<1-65535>	Specifies the index number of the history control interface. The range of values is 1 to 65535.
<ports>	Specifies the port(s) in the port list form: *{slot/port [-slot/port][, ...]}*.
[buckets *<value>*]	Specifies the number of buckets requested. The range of values is 1 to 350. The default is - 50.
[intv *<value>*]	Specifies the time interval in seconds over which the data is sampled for each bucket. The range of values is 1 to 3600. The default is - 1800.
[owner *<LINE>*]	Specifies the name of the owner. The range of values is a string of 1 to 48 characters. The default is cli.

Command mode

Global configuration mode

no rmon history

Use this command to delete the specified history control interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

no rmon history [*<1-65535>* **]**

Variable definitions

Use the following table to help you use the **no rmon history [** *<1-65535>* **]** command.

Variable	Value
<1-65535>	Specifies an optional parameter that specifies the index number for the history control interface. The range of values is 1 to 65535.

rmon memsize

Use this command to specify the amount of Random Access Memory (RAM) in bytes to allocate for the Remote Monitoring (RMON) functions on the switch.

Syntax

rmon memsize *<memsize>*

Variable definitions

Use the following table to help you use the **rmon memsize** *<memsize>* command.

Variable	Value
<memsize>	Specifies the memory size in bytes. The range of values is 250000 to 4000000.

Command mode

Global configuration mode

Comments? infodev@avaya.com

rmon stats

Use this command to create an ether-stats control interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

`rmon stats` <*1-65535*> <*ports*> **`[owner`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`rmon stats`** <*1-65535*> <*ports*> **`[owner`** <*value*> **`]`** command.

Variable	Value
<*1-65535*>	Specifies the index number of the ether-stats control interface. The range of values is 1 to 65535.
<*ports*>	Specifies the port(s) in the port list form: *{slot/port [-slot/port][, ...]}*.
[owner <*value*>]	Specifies the name of the owner. The range of values is a string of 1 to 48 characters.

Command mode

Global configuration mode

no rmon stats

Use this command to delete the specified ether-stats control interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

`no rmon stats [` <*1-65535*> **`]`**

Variable definitions

Use the following table to help you use the **`no rmon stats [`** <*1-65535*> **`]`** command.

Variable	Value
1-65535	Specifies an optional parameter that specifies the index number for the ether-stats control interface. The range of values is 1 to 65535.

Command mode

Global configuration mode

rmon trap-option

Use this command to specify whether the Remote Monitoring (RMON) traps are sent to the owner or all trap recipients.

Syntax

`rmon trap-option {toOwner|toAll}`

Variable definitions

Use the following table to help you use the **`rmon trap-option {toOwner|toAll}`** command.

Variable	Value
toOwner	Specifies to send RMON traps to the owner.
toAll	Specifies to send RMON traps to all trap recipients.

Command mode

Global configuration mode

rmon util-method

Use this command to specify whether port utilization is calculated in half or full duplex for the Remote Monitoring (RMON) functions on the switch.

Syntax

`rmon util-method {half|full}`

Variable definitions

Use the following table to help you use the **`rmon util-method {half|full}`** command.

Variable	Value
half	Specifies that port utilization is calculated in half duplex.
full	Specifies that port utilization is calculated in full duplex.

Command mode

Global configuration mode

test

Use this command to perform a loopback test. The test and show test commands allow you to test an Ethernet Routing Switch 8300while the switch is operating and show the test results. The tests do not interfere with normal bridging and routing activities in the switch, but they do occupy the CPU.

Syntax

`test [loopback` *<port/slot>* **`] [stop loopback`** *<port/slot>* **`]`**

Variable definitions

Use the following table to help you use the **`test`** command.

Variable	Value
loopback *<port/slot>* [*<int|ext>*]	Places the specified ports into internal or external loopback mode. • *portlist* specifies one or more ports, shown as *{ slot/port [- slot/port][,...]}*. • *int|ext* is a string between 1 and 1536.
stop loopback *<port/slot>*	Stops the current loopback test. *ports* specifies one or more ports, shown as *{ slot/port [- slot/port][,...]}*.

Important:

To test a port in loopback mode, put the port into the testing state using the command **`state [port <ports>] test`**. After the test is complete, return the port to its normal mode using the command **`state [port <ports>] enable`**.

Command mode

Privileged EXEC mode

trace auto-enable

Use this command to configure the switch to automatically enable a trace in the event that CPU usage reaches a pre-defined value.

Syntax

trace auto-enable [high-percentage <percent>][high-track-duration <*seconds*> **][low-percentage** <*percent*> **][low-track-duration** <*seconds*> **]**

Variable definitions

Use the following table to help you use the **trace auto-enable [high-percentage <percent>] [high-track-duration** <*seconds*> **] [low-percentage** <*percent*> **] [low-track-duration** <*seconds*> **]** command.

Variable	Value
[high-percentage <*percent*>]	Specifies the percentage of CPU utilization above which auto trace is started. The range of values is 60 to 100. The default is 90.
[high-track-duration <*seconds*>]	Specifies the time in seconds to monitor CPU utilization before triggering a trace. The range of values is 3 to 10. The default is 5.
[low-percentage <*percent*>]	Specifies the percentage of CPU utilization below which auto-trace is stopped. The range of values is 50 to 90. The default is 75.
[low-track-duration <*seconds*>]	Specifies the time in seconds to monitor CPU utilization before disabling the trace. The range of values is 3 to 10. The default is 5.

Important:

The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace auto-enable add-module

Use this command to add a software module to the automatic trace configuration.

Syntax

trace auto-enable add-module <*modid*> <*level*>

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`trace auto-enable add-module`** <*modid*> <*level*> command.

Variable	Value
<*modid*>	Specifies the module to be traced. The range is 0 to 66. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter: `trace auto-enable add-module ?`.
<*level*>	Specifies the level of detail for the trace. The options are: • 0 = Disabled • 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose

Important:

The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace auto-enable auto-trace

Use this command to configure the switch to automatically enable a trace in the event that CPU usage reaches a pre-defined value.

Syntax

`trace auto-enable auto-trace <enable|disable>`

Variable definitions

Use the following table to help you use the **`trace auto-enable auto-trace <enable|disable>`** command.

Variable	Value
enable	Enables auto-trace. The default is disable.
disable	Disables auto-trace. The default is disable.

Important:

The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace auto-enable remove-module

Use this command to remove a module from the automatic trace configuration.

Syntax

`trace auto-enable remove-module` *<modid> <level>*

Variable definitions

Use the following table to help you use the **`trace auto-enable remove-module`** *<modid> <level>* command.

Variable	Value
<modid>	Specifies the module for disabling of auto-trace. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter: `trace auto-enable add-module ?`.
<level>	Specifies the level of the trace. The options are: • 0 = Disabled • 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose

Command mode

Privileged EXEC mode

trace clear

Use this command to clear the trace file.

Comments? infodev@avaya.com

Syntax

`trace clear`

Command mode

Privileged EXEC mode

trace filter

Use this command to filter trace messages.

Syntax

`trace filter`

Command mode

Privileged EXEC mode

trace grep

Use this command to search and extract information from a text string.

Syntax

`trace grep`

Command mode

Privileged EXEC mode

trace level

Use this command to specify the trace level for a software module with the specified module ID. Use **?** to see a list of ID numbers.

Syntax

`trace level [` <*modid*> **`] [`** <*level*> **`]`**

Variable definitions

Use the following table to help you use the **`trace level [`** <*modid*> **`] [`** <*level*> **`]`** command.

Variable	Value
<modid>	Specifies the module to be traced. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter: `trace auto-enable add-module ?`.
<level>	Specifies the level of detail for the trace. The options are: • 0 = Disabled • 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose

Command mode

Privileged EXEC mode

trace off

Use this command to disable tracing on a module.

Syntax

`trace off`

Command mode

Privileged EXEC mode

trace route-policy

Use this command to trace a route policy.

Syntax

`trace route-policy`

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

trace screen

Use this command to display the trace on the screen.

Syntax

`trace screen [` <*setting*> **`]`**

Variable definitions

Use the following table to help you use the **`trace screen [`** <*setting*> **`]`** command.

Variable	Value
<*setting*>	is an optional parameter that specifies whether the trace is displayed on the screen. The options are: on or off.

Command mode

Privileged EXEC mode

traceroute

Use this command to trace the route to a remote host. It is a valuable tool for troubleshooting because it shows all the routes that are used or indicates that the remote network cannot be reached.

Syntax

`traceroute` <*ipaddr*> **`[`** <*datasize*> **`] [-m`** <*value*> **`] [-p`** <*value*> **`] [-q`** <*value*> **`] [-w`** <*value*> **`] [-v]`**

Variable definitions

Use the following table to help you use the **`traceroute`** <*ipaddr*> **`[`** <*datasize*> **`] [-m`** <*value*> **`] [-p`** <*value*> **`] [-q`** <*value*> **`] [-w`** <*value*> **`] [-v]`** command.

Variable	Value
<*ipaddr*>	Specifies the IP address of the remote host.
<*datasize*>	Specifies the size of the probe packet. The range of values is 1 to 1464.
[-m <*value*>]	Specifies the maximum time-to-live (TTL) value. The range of values is 1 to 255.

Variable	Value
[-p <*value*>]	Specifies the base UDP port number. The range of values is 0 to 65535
[-q <*value*>]	Specifies the number of probes per TTL. The range of values is 1 to 255.
[-w <*value*>]	Specifies the wait time per probe. The range of values is 1 to 255.
[-v]	Specifies the verbose mode for displaying extensive trace information.

Command mode

Privileged EXEC mode

vct test

Use this command to configure and enable the Virtual Cable Tester (VCT).

Important:

The following message will appear:

```
WARNING: VCT test will impact the traffic flow. Do you want to continue y/n?
```

Syntax

`vct test` <*ports*>

Variable definitions

Use the following table to help you use the **`vct test`** <*ports*> command.

Variable	Value
<*ports*>	specifies the port(s) in port list form:*{ slot/port [- slot/port][, ...]}*.

Command mode

Global Configuration mode

Comments? infodev@avaya.com

Chapter 13: Multicast services commands

This chapter describes ACLI multicast services commands and their parameters.

Navigation

- debug ip pim on page 349
- interface vlan on page 350
- ip igmp on page 350
- ip igmp access-filter on page 351
- no ip igmp access-filter on page 352
- ip igmp fast-leave on page 354
- no ip igmp fast-leave on page 355
- ip igmp fast-leave-members on page 355
- no ip igmp fast-leave-members on page 355
- ip igmp flush on page 356
- ip igmp immediate-leave-mode on page 357
- default ip igmp immediate-leave-mode on page 357
- ip igmp mrouter on page 357
- no ip igmp mrouter on page 358
- ip igmp multicast-vlan-registration on page 358
- no ip igmp multicast-vlan-registration on page 359
- ip igmp multicast-vlan-registration receiver-vlan on page 359
- no ip igmp multicast-vlan-registration receiver-vlan on page 359
- ip igmp proxy-snoop on page 360
- no ip igmp proxy-snoop on page 360
- ip igmp router-alert on page 361
- no ip igmp router-alert on page 361
- ip igmp snoop on page 361
- no ip igmp snoop on page 362

- ip igmp static-members on page 362
- no ip igmp static-members on page 363
- ip igmp on page 363
- no ip igmp on page 365
- default ip igmp on page 368
- ip igmp generate-log on page 370
- no ip igmp generate-log on page 370
- default ip igmp generate-log on page 370
- ip igmp generate-trap on page 371
- no ip igmp generate-trap on page 371
- default ip igmp generate-trap on page 371
- ip igmp mrdisc on page 372
- no ip igmp mrdisc on page 372
- default ip igmp mrdisc on page 373
- ip igmp snoop-querier on page 373
- no ip igmp snoop-querier on page 373
- ip igmp snoop-querier-addr on page 373
- no ip igmp snoop-querier-addr on page 374
- ip igmp stream-limit on page 377
- no ip igmp stream-limit on page 378
- ip igmp stream-limit-group enable max-streams on page 378
- no ip igmp stream-limit-group on page 379
- default ip igmp stream-limit-group on page 379
- ip igmp stream-limit-max-streams on page 380
- ip mroute static-source-group on page 380
- no ip mroute static-source-group on page 381
- ip pim on page 382
- no ip pim on page 385
- ip pim enable on page 385
- ip pim interface virtual neighbor on page 386
- no ip pim interface virtual neighbor on page 387
- ip pim rp-candidate group rp on page 387
- no ip pim rp-candidate group rp on page 388
- ip pim static-rp on page 388

- no ip pim static-rp on page 389
- ip pim static-rp on page 389
- no ip pim static-rp on page 390

debug ip pim

Use this command to configure PIM-SM protocol traces for troubleshooting.

Syntax

`debug ip pim`

Variable definitions

The following table describes variables that help you use the **`debug ip pim`** command.

Variable	Value
assert / no debug ip pim assert	Allows you to set the switch to display the assert debug traces
bstrap /no debug ip pim bstrap	Allows you to set the switch to display bootstrap debug traces.
group<*ipaddress*>	Allows you to set the switch to display debug traces from a specific group ip-address.
hello / no debug ip pim hello	Allows you to set the switch to display hello debug traces.
joinprune /no debug ip pim joinprune	Allows you to set the switch to display join/ prune debug traces.
pimdbgtrace /no debug ip pim pimdbgtrace	Allows you to set the switch to display PIM-SM debug traces.
pimdbglog /no debug ip pim pimdbglog	Allows you to control whether the switch logs debug traces.
register /no debug ip pim register	Allows you to set the switch to display register debug traces.
regstop /no ip debug ip pim regstop	Allows you to set the switch to display register stop debug traces.
rp-adv / no debug ip pim rp-adv	Allows you to set the switch to display rp advertisement debug traces.
send-trace /no debug ip pim send-trace	Allows you to set the switch to display send debug traces.
rcv-dbg-trace /no debug ip pim rcv-dbg-trace	Allows you to set the switch to display received debug traces.

Variable	Value
source<*ipaddress*>	Allows you to set the switch to display debug traces from a specific source ip-address.

Command mode

Global configuration mode

interface vlan

Use this command to access the interface on a Virtual LAN (VLAN).

Syntax

`interface vlan <vid>`

Variable definitions

Use the following table to help you use the **`interface vlan <vid>`** command.

Variable	Value
vid	Specifies a VLAN ID from 1 to 4000. (Note that 1 to 2000 is the default, while 1 to 4000 is valid when the vid-max4k flag is set to true).

Command mode

Interface configuration mode

ip igmp

Use this command to configure the Internet Group Management Protocol (IGMP) interface on a VLAN.

Syntax

`ip igmp [last-member-query-int] [query-interval` <*seconds*> **`] [query-max-resp`** <*1/10 seconds*> **`] [robustval`** <*integer*> **`] [version`** <*integer*> **`]`**

Variable definitions

Use the following table to help you use the **`ip igmp [last-member-query-int] [query-interval`** <*seconds*> **`] [query-max-resp`** <*1/10 seconds*> **`] [robustval`** <*integer*> **`] [version`** <*integer*> **`]`** command.

Comments? infodev@avaya.com

Variable	Value
fast-leave-members>*slot/port*>	If you enable fast-leave, this parameter configures IGMP fast-leave members.
[query-interval <*seconds*>]	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. *seconds* is the range from 1 to 65535. The default value is 125 seconds.
[query-max-resp <*1/10 seconds*>]	Sets the maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This field is a read-only field and is not supported in the Ethernet Routing Switch 8300.
[robustval <*integer*>]	Allows tuning for the expected packet loss on a network. *integer* is an integer value with a range of 2 to 255 seconds. The default value is 2 seconds. Increase the value if you expect the network to experience loss.
[version <*integer*>]	Sets the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. *integer* is an integer value with a value of 1-3. The default value is 2 (IGMPv2).

Command mode

Interface configuration mode

ip igmp access-filter

Use this command to configure the access filter for multicast access control on a selected IGMP interface for a specific multicast group.

Syntax

`ip igmp access-filter` <*grpAddr*> <*hostAddr*> <*hostMask*> **`<denyRX|denyBoth>`**

Variable definitions

Use the following table to help you use the **`ip igmp access-filter`** <*grpAddr*> <*hostAddr*> <*hostMask*> **`<denyRX|denyBoth>`** command.

Variable	Value
<grpAddr>	Specifies the selected multicast group.
<hostAddr>	Specifies the IP address of the host route.
<hostMask>	Specifies the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host's network.
<denyRX|denyBoth>	Allows you to create access filters for the Ethernet Routing Switch 8300. The denyRX filter prevents the switch from receiving IGMP reports from a particular client. The denyBoth filter prevents the switch from receiving IGMP reports and forwarding datagram traffic for a particular multicast group on the VLAN.

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

no ip igmp access-filter

Use this command to delete the access-filter group entry for a selected IGMP interface.

Syntax

`no ip igmp access-filter` *<grpAddr> <hostAddr> <hostMask> <denyRX|denyBoth>*

Variable definitions

Use the following table to help you use the **`no ip igmp access-filter`** *<grpAddr> <hostAddr> <hostMask> <denyRX|denyBoth>* command.

Variable	Value
<grpAddr>	Deletes the selected multicast group.
<hostAddr>	Deletes the IP address of the host route.
<hostMask>	Deletes the subnet mask used to determine the host or hosts covered by this configuration.
<denyRX>|<denyBoth>	Deletes the denyRX or denyBoth access filters.

Comments? infodev@avaya.com

Command mode

Interface configuration mode

ip igmp compatibility-mode

Use this command to enable the compatibility mode on a VLAN.

Syntax

ip igmp compatibility-mode

Command mode

VLAN Interface Configuration mode

no ip igmp compatibility-mode

Use this command to disable the compatibility mode on a VLAN.

Syntax

no ip igmp compatibility-mode

Command mode

VLAN Interface Configuration mode

default ip igmp compatibility-mode

Use this command to configure the default compatibility mode on a VLAN.

Syntax

default ip igmp compatibility-mode

Command mode

VLAN Interface Configuration mode

ip igmp dynamic-downgrade-version

Use this command to enable the dynamic downgrade version on a VLAN.

Syntax

ip igmp dynamic-downgrade-version

Command mode

VLAN Interface Configuration mode

no ip igmp dynamic-downgrade-version

Use this command to disable the dynamic downgrade version on a VLAN.

Syntax

no ip igmp dynamic-downgrade-version

Command mode

VLAN Interface Configuration mode

default ip igmp dynamic-downgrade-version

Use this command to configure the dynamic downgrade version on a VLAN to the default value.

Syntax

default ip igmp dynamic-downgrade-version

Command mode

VLAN Interface Configuration mode

ip igmp fast-leave

Use this command to enable a given port to recognize an IGMPv2 leave message. This causes the group member to be immediately flushed from the IGMP table. Note that this is differs from IGMPv1 behavior where entries in the IGMP table must age out using the expiration timer.

Syntax

ip igmp fast-leave

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

no ip igmp fast-leave

Use this command to disable a given port from receiving a leave message from any IGMP member in any given group.

Syntax

no ip igmp fast-leave

Command mode

Interface configuration mode

ip igmp fast-leave-members

Use this command to enable IGMP fast-leave members on a VLAN.

Syntax

ip igmp fast-leave-members <*slot/port*>

Variable definitions

Use the following table to help you use the **ip igmp fast-leave-members** <*slot/port*> command.

Variable	Value
<*slot/port*>	specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

no ip igmp fast-leave-members

Use this command to disable IGMP fast-leave members on a VLAN.

Syntax

no ip igmp fast-leave-members <*slot/port*>

Variable definitions

Use the following table to help you use the **no ip igmp fast-leave-members** <*slot/port*> command.

Variable	Value
<*slot/port*>	specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*

Command mode

Interface configuration mode

ip igmp flush

Use this command to flush the specified table for the IGMP interface.

Syntax

ip igmp flush <*mrouter*|*sender*|*grp-member*> <*sender ipaddress*> <*group ipaddress*>

Variable definitions

Use the following table to help you use the **ip igmp flush** <*mrouter*|*sender*|*grp-member*> <*sender ipaddress*> <*group ipaddress*> command.

Variable	Value
<mrouter> <sender ipaddress> <group ipaddress>	Specifies the selected multicast router.
<sender> <sender ipaddress> <group ipaddress>	Specifies the selected sender.
<grp-member> <sender ipaddress> <group ipaddress>	Specifies the selected multicast group member.

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

Comments? infodev@avaya.com

ip igmp immediate-leave-mode

Use this command to set the immediate leave mode.

Syntax

`ip igmp immediate-leave-mode <multiple-user|one-user mode>`

Variable definitions

Use the following table to help you use the **`ip igmp immediate-leave-mode <multiple-user|one-user mode>`** command.

Variable	Value
<multiple-user|one-user mode>	specifies the immediate leave mode as multiple user or one user.

Command mode

Global configuration mode

default ip igmp immediate-leave-mode

Use this command to set the immediate leave mode to the default setting.

Syntax

`default ip igmp immediate-leave-mode`

Command mode

Global configuration mode

ip igmp mrouter

Use this command to add IGMP multicast router ports on a VLAN.

Syntax

`ip igmp mrouter` <*slot/port*>

Variable definitions

Use the following table to help you use the **`ip igmp mrouter`** <*slot/port*> command.

Variable	Value
slot/port	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Interface configuration mode

For more information about IGMP operations, see *Configuring IP Multicast Routing Protocols*.

no ip igmp mrouter

Use this command to delete IGMP multicast router ports on a VLAN.

Syntax

`no ip igmp mrouter` <*slot/port*>

Variable definitions

Use the following table to help you use the **`no ip igmp mrouter`** <*slot/port*> command.

Variable	Value
slot/port	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Interface configuration mode

ip igmp multicast-vlan-registration

Use this command to configure MVR to save bandwidth and maintain the performance of the multicast router when multicast groups are located in different VLANs.

syntax

`ip igmp multicast-vlan-registration`

Command mode

Global configuration mode

Comments? infodev@avaya.com

no ip igmp multicast-vlan-registration

Use this command to disable MVR so that you can enable PIM.

syntax

`no ip igmp multicast-vlan-registration`

Command mode

Global configuration mode

ip igmp multicast-vlan-registration receiver-vlan

Use this command to add a receiver VLAN to the MVR VLAN to bind the VLAN.

syntax

`ip igmp multicast-vlan-registration receiver-vlan <1-4000>`

Variable definitions

Use the data in the following table to help you use **`ip igmp multicast-vlan-registration receiver-vlan`** command.

Variable	Value
receiver vlan <1-4000>	Specifies a VLAN containing a receiver. <1—4000> is the identifier for the VLAN. Values range from 1 to 4000.

Command mode

Global configuration mode

no ip igmp multicast-vlan-registration receiver-vlan

Use this command to remove a receiver VLAN to the MVR VLAN to unbind the VLAN.

syntax

`no ip igmp multicast-vlan-registration receiver-vlan <1-4000>`

Variable definitions

Use the data in the following table to help you use **no ip igmp multicast-vlan-registration receiver-vlan** command.

Variable	Value
receiver vlan <1-4000>	Specifies a VLAN containing a receiver. <1—4000> is the identifier for the VLAN. Values range from 1 to 4000.

Command mode

Global configuration mode

ip igmp proxy-snoop

Use this command to enable the proxy-snoop option for the VLAN. When IGMP report messages come from different clients, all of these messages are sent to the IGMP querier. If you enable IGMP proxy snoop, then only one report message is sent to the querier for that group. As a result, this command allows you to suppress control messages going to the CPU.

Syntax

ip igmp proxy-snoop

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

no ip igmp proxy-snoop

Use this command to disable the proxy-snoop option for the VLAN.

Syntax

no ip igmp proxy-snoop

Command mode

Interface configuration mode

Comments? infodev@avaya.com

ip igmp router-alert

Use this command to enable the router alert feature. When enabled, it instructs the Ethernet Routing Switch 8300to drop packets without the router-alert flag in the IP header.

Syntax

ip igmp router-alert

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

no ip igmp router-alert

Use this command to disable the router alert feature.

Syntax

no ip igmp router-alert

Command mode

Interface configuration mode.

ip igmp snoop

Use this command to enable the snoop option for the VLAN. When multicast data enters a Layer 2 VLAN, data packets are flooded to all ports in that VLAN. If you enable IGMP snoop on the VLAN, these packets are only forwarded to the ports on which the IGMP joins have been received. In other words, data packets are forwarded only on the multicast client ports.

Syntax

ip igmp snoop

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)*.

no ip igmp snoop

Use this command to disable the snoop option for the VLAN.

Syntax

no ip igmp snoop

Command mode

Interface configuration mode

ip igmp static-members

Use this command to create IGMP static members on a VLAN.

Syntax

ip igmp static-members *<group-address> add-ports remove-ports <slot/port> static|blocked*

Variable definitions

Use the following table to help you use the **ip igmp static-members** *<group-address> add-ports remove-ports <slot/port> static|blocked* command.

Variable	Value
<group-address>	Specifies the IP address of the selected multicast group.
add-ports	Specifies that you wish to add ports to the created static group entry.
remove-ports	Specifies that you wish to remove ports from the created static group entry.
<slot/port>	Specifies the ports you wish to create static members for in the following form: {slot/port [-slot/port][, ...]}
static|blocked	Designates the route as static or blocked.

Command mode

Interface configuration mode

For more information about IGMP operations, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using ACLI and CLI (NN46200-500)* and

Comments? infodev@avaya.com

Avaya Ethernet Routing Switch 8300 Configuration — Security using CLI and ACLI (NN46200-503).

no ip igmp static-members

Use this command to delete IGMP static members on a VLAN.

Syntax

`no ip igmp static-members` <*group-address*>

where <*group-address*> specifies the IP address of the selected multicast group.

Command mode

Interface configuration mode

ip igmp

Use this command to configure IGMP on a VLAN.

Syntax

`ip igmp`

Variable definitions

The following table describes variables that you enter after the **`ip igmp`** command.

Variable	Value
access-list WORD <1-64> <HostAddress> <MaskAddress> <deny-tx|deny-rx|deny-both|allow-only-tx|allo w-only-rx|allow-only-both>	Sets the IP multicast access group list parameters. • <*1-64*> is an IP prefix-list entry name in a 1 to 64 character string. • <deny-tx|deny-rx|deny-both|allow-only-tx| allo w-only-rx|allow-only-both> indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.
immediate-leave	Enables IGMP immediate-leave mode on the interface. The default is enabled.
immediate-leave-members {slot/port [-slot/port][, ...]}	If you enable immediate-leave, this parameter configures IGMP immediate-leave members. The default is added.

Variable	Value
last-member-query-interval	Configures the IGMP last member query interval (in 1/10 seconds). .
mrouter {slot/port [-slot/port][, ...]}	Adds multicast router ports. **Important:** When IGMP join or multicast data ingress to an Ethernet Routing Switch 8300snoop VLAN port, they are only forwarded upstream via the querier port. You can use this parameter to create your own mrouter ports statically. After you create static mrouter ports, join and data are also forwarded to these static mrouter ports.
proxy	Enables the proxy option for the VLAN. **Important:** When IGMP report messages come from different clients, all of these messages are sent to the querier. If you enable IGMP proxy snoop, then only one report message is sent to the querier for that group. As a result, this parameter allows you to suppress control messages going to the CPU.
query-interval	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. **Important:** In the case of IGMP snoop, be sure that the query-interval is configured the same as the multicast router (IGMP querier).
query-max-response <0-255>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.
robust-value	Allows tuning for the expected packet loss on a network. **Important:** In the case of IGMP snoop, be sure that the robustval parameter is configured the same as the multicast router (IGMP querier).
router-alert	Enables the router alert feature. When enabled, this parameter instructs the router to drop packets without the router-alert flag in the IP header.

Variable	Value
	Important: To maximize your network performance, Avaya recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable (not supported in the Ethernet Routing Switch 8300)
snooping	Enables the snooping option for the VLAN. **Important:** When multicast data enters a Layer 2 VLAN, data packets are flooded to all ports in that VLAN. If you enable IGMP snoop on the VLAN, these packets are only forwarded to the ports on which IGMP joins have been received. In other words, data packets are forwarded only on multicast client ports.
static-group <groupAddress> port {slot/port[-slot/port][,...]} <static|blocked>	Configures IGMP static members on a VLAN. The Ethernet Routing Switch 8300allows you to configure static receivers, or members, for given multicast groups on specific VLANs using the VLAN IP address. Static receivers allow multicast traffic to be sent for the configured groups on the VLAN without IGMP receivers having to be attached to this VLAN.
version <1|2>	Specifies the version of IGMP as IGMPv1 or IGMPv2. The default is IGMPv2.

Command mode

Interface VLAN mode

no ip igmp

Use the following command to disable IGMP features on a VLAN.

Syntax

`no ip igmp`

Variable definitions

The following table describes variables that you enter after the **no ip igmp** command.

Variable	Value
access-list WORD <1-64> <HostAddress> <MaskAddress> <deny-tx|deny-rx|deny-both|allow-only-tx|allo w-only-rx|allow-only-both>	Sets the IP multicast access group list parameters. • *<1-64>* is an IP prefix-list entry name in a 1 to 64 character string. • <deny-tx|deny-rx|deny-both|allow-only-tx| allo w-only-rx|allow-only-both> indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.
immediate-leave	Enables IGMP immediate-leave mode on the interface. The default is enabled.
immediate-leave-members {slot/port [-slot/port][, ...]}	If you enable immediate-leave, this parameter configures IGMP immediate-leave members. The default is added.
last-member-query-interval	Configures the IGMP last member query interval (in 1/10 seconds). .
mrouter {slot/port [-slot/port][, ...]}	Adds multicast router ports. **Important:** When IGMP join or multicast data ingress to an Ethernet Routing Switch 8300snoop VLAN port, they are only forwarded upstream via the querier port. You can use this parameter to create your own mrouter ports statically. After you create static mrouter ports, join and data are also forwarded to these static mrouter ports.
proxy	Enables the proxy option for the VLAN. **Important:** When IGMP report messages come from different clients, all of these messages are sent to the querier. If you enable IGMP proxy snoop, then only one report message is sent to the querier for that group. As a result, this parameter allows you to suppress control messages going to the CPU.
query-interval	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN.

Comments? infodev@avaya.com

Variable	Value
	Important: In the case of IGMP snoop, be sure that the query-interval is configured the same as the multicast router (IGMP querier).
query-max-response <0-255>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.
robust-value	Allows tuning for the expected packet loss on a network. **Important:** In the case of IGMP snoop, be sure that the robustval parameter is configured the same as the multicast router (IGMP querier).
router-alert	Enables the router alert feature. When enabled, this parameter instructs the router to drop packets without the router-alert flag in the IP header. **Important:** To maximize your network performance, Avaya recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable (not supported in the Ethernet Routing Switch 8300)
snooping	Enables the snooping option for the VLAN. **Important:** When multicast data enters a Layer 2 VLAN, data packets are flooded to all ports in that VLAN. If you enable IGMP snoop on the VLAN, these packets are only forwarded to the ports on which IGMP joins have been received. In other words, data packets are forwarded only on multicast client ports.
static-group <groupAddress> port {slot/port[-slot/port][,...]} <static|blocked>	Configures IGMP static members on a VLAN. The Ethernet Routing Switch 8300allows you to configure static receivers, or members, for given multicast groups on specific VLANs using the VLAN IP address.

Variable	Value
	Static receivers allow multicast traffic to be sent for the configured groups on the VLAN without IGMP receivers having to be attached to this VLAN.
version <1|2>	Specifies the version of IGMP as IGMPv1 or IGMPv2. The default is IGMPv2.

Command mode

Interface VLAN mode

default ip igmp

Use this command to set the IGMP parameters to the default values

Syntax

`default ip igmp`

Variable definitions

Use the following table to help you use the **`default ip igmp`** command.

Variable	Value
access-list WORD<1-64> <HostAddress> <MaskAddress> <deny-tx|deny-rx|deny-both|allow-only-tx|allo w-only-rx|allow-only-both>	Sets the IP multicast access group list parameters to default values. • *<1-64>* is an IP prefix-list entry name in a 1 to 64 character string. • <deny-tx|deny-rx|deny-both|allow-only-tx|allo w-only-rx|allow-only-both> indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.
immediate-leave	Enables IGMP immediate-leave mode on the interface. The default is enabled.
immediate-leave-members {slot/port [-slot/port][, ...]}	If you enable immediate-leave, this parameter configures IGMP immediate-leave members. The default is added.
last-member-query-interval	Configures the IGMP last member query interval (in 1/10 seconds).
proxy	Enables the proxy option for the VLAN.

Comments? infodev@avaya.com

Variable	Value
	Important: When IGMP report messages come from different clients, all of these messages are sent to the querier. If you enable IGMP proxy snoop, then only one report message is sent to the querier for that group. As a result, this parameter allows you to suppress control messages going to the CPU.
query-interval	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. **Important:** In the case of IGMP snoop, be sure that the query-interval is configured the same as the multicast router (IGMP querier).
query-max-response <0-255>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.
robust-value	Allows tuning for the expected packet loss on a network. **Important:** In the case of IGMP snoop, be sure that the robustval parameter is configured the same as the multicast router (IGMP querier).
router-alert	Enables the router alert feature. When enabled, this parameter instructs the router to drop packets without the router-alert flag in the IP header. **Important:** To maximize your network performance, Avaya recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable (not supported in the Ethernet Routing Switch 8300)
snooping	Enables the snooping option for the VLAN.

Variable	Value
	Important: When multicast data enters a Layer 2 VLAN, data packets are flooded to all ports in that VLAN. If you enable IGMP snoop on the VLAN, these packets are only forwarded to the ports on which IGMP joins have been received. In other words, data packets are forwarded only on multicast client ports.
default ip igmp version	Sets IGMP to the default version. The default is IGMPv2.

Command mode

Interface VLAN mode

ip igmp generate-log

Use this command to configure on IGMP generate log.

Syntax

`ip igmp generate-log`

Command mode

Global configuration mode

no ip igmp generate-log

Use this command to disable an IGMP generate log.

Syntax

`no ip igmp generate-log`

Command mode

Global configuration mode

default ip igmp generate-log

Use this command to set an IGMP generate log to default values.

Syntax

default ip igmp generate-log

Command mode

Global configuration mode

ip igmp generate-trap

Use this command to configure an IGMP generate trap.

Syntax

ip igmp generate-trap

Command mode

Global configuration mode

no ip igmp generate-trap

Use this command to disable an IGMP generate log.

Syntax

no ip igmp generate-trap

Command mode

Global configuration mode

default ip igmp generate-trap

Use this command to set an IGMP generate log to default values.

Syntax

default ip igmp generate-trap

Command mode

Global configuration mode

ip igmp mrdisc

Use this command to configure multicast router discovery parameters on a VLAN.

Syntax

`ip igmp mrdisc`

Variable definitions

Use the following table to help you use the **`ip igmp mrdisc`** command.

Variable	Value
<cr>	Enables multicast router discovery parameters on a VLAN. <cr> is a carriage return.
maxadvertinterval <value>	Specifies the maximum interval in seconds between successive advertisements.
maxinitadvertinterva<value>	Specifies the maximum advertisement interval in seconds between successive initial advertisements.
maxinitadvertisements <value>	Specifies the maximum advertisements after initialization.
minadvertinterval <value>	Specifies the minimum interval in seconds between successive advertisements.
neighdeadinterval <value>	Specifies the maximum time in seconds allowed before a neighbor is declared dead.

Command mode

Interface VLAN mode

no ip igmp mrdisc

Use this command to disable multicast router discovery on a VLAN.

Syntax

`no ip igmp mrdisc`

Command mode

Interface VLAN mode

default ip igmp mrdisc

Use this command to set the default values for multicast router discovery on a VLAN.

Syntax

`default ip igmp mrdisc`

Command mode

Interface VLAN mode

ip igmp snoop-querier

Use this command to enable IGMP snoop querier.

Syntax

`ip igmp snoop-querier`

Command mode

Interface VLAN mode

no ip igmp snoop-querier

Use this command to disable IGMP snoop querier.

Syntax

`no ip igmp snoop-querier`

Command mode

Interface VLAN mode

ip igmp snoop-querier-addr

Use this command to configure the source IP address used in the query message.

Syntax

`ip igmp snoop-querier-addr`

Variable definitions

Use the following table to help you use the **ip igmp snoop-querier-addr** command.

Variable	Value
<ipaddr>	Specifies the source IP address used in the query message.

Command mode

Interface VLAN mode

no ip igmp snoop-querier-addr

Use this command to return the source IP address to the default value, 0.0.0.0.

Syntax

no ip igmp snoop-querier-addr

Command mode

Interface VLAN mode

ip igmp ssm dynamic-learning

Use this command to enable SSM dynamic learning.

Syntax

ip igmp ssm dynamic-learning

Command mode

Global Configuration mode

no ip igmp ssm dynamic-learning

Use this command to disable SSM dynamic learning.

Syntax

no ip igmp ssm dynamic-learning

Command mode

Global Configuration mode

default ip igmp ssm dynamic-learning

Use this command to configure SSM dynamic learning to the default value (enable).

Syntax

default ip igmp ssm dynamic-learning

Command mode

Global Configuration mode

ip igmp ssm group-range

Use this command to configure the SSM range.

Syntax

ip igmp ssm group-range *[A.B.C.D/<0-32>]*

[A.B.C.D/<0-32>] identifies the source IP address and address mask value.

Command mode

Global Configuration mode

ip igmp ssm-map

Use this command to configure the SSM channel to generate an IGMPv3 report packet.

Syntax

ip igmp ssm-map <IP Address> <source IP Address>

Command mode

Global Configuration mode

ip igmp ssm-map enable

Use this command to enable the SSM channel entry.

Syntax

ip igmp ssm-map <A.B.C.D> enable

<*A.B.C.D*> identifies the group IP address.

Command mode

Global Configuration mode

no ip igmp ssm-map enable

Use this command to disable the SSM channel entry.

Syntax

no ip igmp ssm-map <A.B.C.D> enable

<*A.B.C.D*> identifies the group IP address.

Command mode

Global Configuration mode

no ip igmp ssm-map

Use this command to delete a SSM channel entry.

Syntax

no ip igmp ssm-map <A.B.C.D>

<*A.B.C.D*> identifies the group IP address.

Command mode

Global Configuration mode

ip igmp ssm-map all

Use this command to enable all the entries in the ssm-channel.

Syntax

`ip igmp ssm-map all`

Command mode

Global Configuration mode

no ip igmp ssm-map all

Use this command to disable all the entries in the ssm-channel.

Syntax

`no ip igmp ssm-map all`

Command mode

Global Configuration mode

ip igmp stream-limit

Use this command to configure multicast stream limitation on a VLAN.

Syntax

`ip igmp stream-limit`

Variable definitions

Use the following table to help you use the **`ip igmp stream-limit`** command.

Variable	Value
<cr>	Enables mulitcast stream limitation on a VLAN. <cr> is carriage return.

Variable	Value
stream-limit-max-streams <value>	Sets the maximum number of streams allowed on an interface. <value> is an integer in a range from 0 to 65535 and the default is 4.

Command mode

Interface VLAN mode

no ip igmp stream-limit

Use this command to disable multicast stream limitation an a VLAN.

Syntax

no ip igmp stream-limit

Command mode

Interface VLAN mode

ip igmp stream-limit-group enable max-streams

Use this command to enable the multicast stream limit group and set the mximum streams.

Syntax

ip igmp stream-limit-group <ports> enable max-streams <value>

- is a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.
- .

Variable definitions

Use the following table to help you use the **ip igmp stream-limit-group <ports> enable max-streams <value>** command.

Variable	Value
<value>	sets the maximum number of streams allowed on an interface. The range is from 0 to 65535, and the default is 4.

Variable	Value
<ports>	Specifies a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.

Command mode

Interface VLAN mode

no ip igmp stream-limit-group

Use this command to disable a multicast stream limit member.

Syntax

no ip igmp stream-limit-group <ports>

Variable definitions

Use the following table to help you use the **no ip igmp stream-limit-group <ports>** command.

Variable	Value
<ports>	Specifies a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.

Command mode

Interface VLAN mode

default ip igmp stream-limit-group

Use this command to set a multicast stream limit group parameters to the default values.

Syntax

default ip igmp stream-limit-group <ports>

Variable definitions

Use the following table to help you use the **default ip igmp stream-limit-group <ports>** command.

Variable	Value
<ports>	Specifies a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.

ip igmp stream-limit-max-streams

Use this command to configure the stream limitation maximum streams.

Syntax

`ip igmp stream-limit-max-streams <0-65535>`

Variable definitions

Use the following table to help you use the **`ip igmp stream-limit-max-streams`** command.

Variable	Value
<0-65535>	Specifies the value of the maximum streams.

Command mode

Interface VLAN mode

default ip igmp stream-limit-max-streams

Use this command to set the stream imitation maximum streams to the default values.

Syntax

`default ip igmp stream-limit-max-streams`

Command mode

Interface VLAN mode

ip mroute static-source-group

Use this command to add a static source-group entry to the PIM multicast routing table.

Comments? infodev@avaya.com

Syntax

ip mroute static-source-group <A.B.C.D> <A.B.C.D/0-32>

Variable definitions

Use the following table to help you use the **ip mroute static-source-group <A.B.C.D> <A.B.C.D/0-32>** command.

Variable	Value
<A.B.C.D>	Specifies the multicast source address for this static source-group entry. How you configure the source address depends on the protocol you are using and in what mode.
<A.B.C.D/0-32>	Specifies the subnet mask of the source for this static source-group entry.

Command mode

Global configuration mode

no ip mroute static-source-group

Use this command to remove a static source-group entry from the PIM multicast routing table.

Syntax

no ip mroute static-source-group <A.B.C.D> <A.B.C.D/0-32>

Variable definitions

Use the following table to help you use the **no ip mroute static-source-group <A.B.C.D> <A.B.C.D/0-32>** command.

Variable	Value
<A.B.C.D>	Specifies the multicast source address for this static source-group entry. How you configure the source address depends on the protocol you are using and in what mode.
<A.B.C.D/0-32>	Specifies the subnet mask of the source for this static source-group entry.

ip pim

Use this command to:

- configure PIM-SM globally.
- configure PIM-SM on a VLAN

Configuring PIM-SM globally

Use this command to configure PIM-SM globally on a switch.

Syntax

`ip pim`

Variable definitions

Use the following table to help you use the **`ip pim`** command.

Variable	Value
bootstrap-period<*integer*>	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. *integer* is an integer in the range of 5–32757. The default is 60.
rp-c-adv-timeout<*integer*>	Specifies how often (in seconds) that routers configured as candidate RPs send C-RP advertisement messages. When this timer expires, the C-RP sends an advertisement message to the elected BSR. *integer* is an integer in the range of 5–26214. The default is 60.
disc-data-timeout <*integer*>	Specifies how long (in seconds) to discard data until the Join is received from the RP. An ipmc discard record is created after a register packet is sent, until the the timer expires or when a Join is received. *integer* is an integer in the range of 5–65535. The default is 60.
activity-chk-interval <15|30|210>	Specifies how often (in seconds) to check traffic activity for a multicast group. The lower

Comments? infodev@avaya.com

Variable	Value
	the value, the more often the switch checks the activity. The default is 210. Notes: • Before you can change the activity-chk-interval, you must disable PIM-SM globally. • Avayal recommends an activity check interval of 30 seconds. • Avaya recommends that you set the activity check interval to 210 seconds for systems that have a large number (200+) of S,G streams. • When one of the timer activity-chk-interval or fwd-cache-timeout is configured with a nondefault value, the other cannot be configured.
join-prune-interval <*integer*>	Specifies how long to wait (in seconds) before the PIM-SM router sends out the next join/prune message to its upstream neighbors. *integer* is an integer in the range of 1–18724. The default is 60.
fwd-cache-timeout<*integer*>	Configures the forward cache timeout globally. The default is 210 *integer*is an integer in the range 10–86400. The default is 210
register-suppression-timeout <*integer*>	Sets the PIM-SM register suppression timeout. The default is 60. *integer*is an integer in the range 6–65535. The default is 60
unicast-route-change-timeout <*integer*>	Sets the PIM-SM unicast route change timeout. *integer*is an integer in the range 2–65535. The default is 5.

Command mode

Global configuration mode

Configuring PIM-SM on a VLAN

Use this command to configure PIM-SM on a VLAN.

Syntax

`ip pim`

Variable definitions

Use the following table to help you use the **`ip pim`** command.

Variable	Value
bsr-candidate preference <*integer*>	Enables the BSR candidate. *integer* is an integer with a range of 0 to 255. The default is -1, which indicates that the current interface is not a Candidate BSR
enable	Enables PIM on a particular VLAN.
interface-type <active|passive>	Sets the interface type on a particular VLAN. • active allows PIM-SM control traffic to be transmitted and received. • passivepassive prevents PIM-SM control traffic from being transmitted or received, thereby reducing the load on a system. This feature is useful when a high number of PIM-SM interfaces exist and are connected to end users, not to other switches.
join-prune-interval<*seconds*>	Specifies how long to wait (in seconds) before the PIM-SM switch sends out the next join/prune message to its upstream neighbors. The range is 1 to 18724 seconds and the default is 60 seconds.
query-interval<*seconds*>	Sets the hello interval to a particular VLAN. The range is 0 to 18724 seconds and the default is 30 seconds.

Command mode

Interface VLAN mode

Comments? infodev@avaya.com

ip pim enable

Use this command to:

- enable Protocol Independent Multicast-Sparse Mode (PIM-SM) globally.
- enable PIM-SM on a selected VLAN

  When you enable PIM-SM on a selected VLAN, you must also enable it globally.

Enabling PIM-SM globally

You can use this command to enable PIM globally on the switch

Syntax

`ip pim enable`

Command mode

Global configuration mode

Enabling PIM-SM on a VLAN

You can use this command to enable PIM on a VLAN.

Syntax

`ip pim enable`

no ip pim

Use this command to:

- disable PIM-SM globally.
- disable PIM-SM on a VLAN

Disabling PIM-SM globally

You can use this command to disable PIM globally on the switch

Syntax

no ip pim

Command mode

Global configuration mode

Disabling PIM-SM on a VLAN

You can use this command to disable PIM on a VLAN.

Syntax

no ip pim

Command mode

Interface VLAN mode

ip pim interface virtual neighbor

Use this command to enable a virtual neighbor. A virtual neighbor is a PIM-SM neighbor IP address on the Ethernet Routing Switch 8300 neighbor table. A virtual neighbor is typically used where the next-hop for a static route cannot run PIM-SM, such as the virtual VRRP address on an adjacent device.

Syntax

ip pim interface <ipaddr> virtual-neighbor <ipaddr>

Variable definitions

Use the following table to help you use the **ip pim interface <ipaddr> virtual-neighbor <ipaddr>** command.

Variable	Value
<ipaddr>	Specifies the IP address of the virtual neighbor.
<ipaddr>	Specifies the IP address of the interface.

Comments? infodev@avaya.com

Command mode

Global configuration mode

no ip pim interface virtual neighbor

Use this command to disable a virtual neighbor.

Syntax

no ip pim interface <ipaddr> virtual-neighbor

Variable definitions

Use the following table to help you use the **ip pim interface <ipaddr> virtual-neighbor <ipaddr>** command.

Variable	Value
<ipaddr>	Specifies the IP address of the interface.

ip pim rp-candidate group rp

Use this command to add a rendezvous point (RP) in the RP set.

Syntax

ip pim rp-candidate group<ipaddr> <mask> rp <ipaddr>

Variable definitions

Use the following table to help you use the **ip pim rp-candidate group<ipaddr> <mask> rp <ipaddr>** command.

Variable	Value
<ipaddr>	Specifies the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
<mask>	Specifies the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.
<ipaddr>	Specifies the IP address of the C-RP. This address must be one of the local PIM-SM enabled interfaces.

Command mode

Global configuration mode

no ip pim rp-candidate group rp

Use this command to remove a rendezvous point (RP) in the RP set.

Syntax

no ip pim rp-candidate group <ipaddr> <mask>

Variable definitions

Use the following table to help you use the **no ip pim rp-candidate group <ipaddr> <mask>** command.

Variable	Value
<ipaddr>	Specifies the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
<mask>	Specifies the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.

Command mode

Gobal configuration mode

ip pim static-rp

Use this command to enable a static RP.

Syntax

ip pim static-rp

When you enter this command, the following message appears:

```
WARNING: RP information learnt dynamically through BSR functionality will be lost.

Do you wish to enable Static RP? (y/n) ?
```

Command mode

Global configuration mode

Comments? infodev@avaya.com

no ip pim static-rp

Use this command to disable a static RP.

Syntax

no ip pim static-rp

When you enter this command, the following message appears:

```
WARNING: Static RP information will be lost.

Do you wish to disable Static RP? (y/n) ?
```

Command mode

Global configuration mode

ip pim static-rp

Use this command to add a static RP to the RP set.

Syntax

ip pim static-rp <group> <mask> <rp>

Variable definitions

Use the following table to help you use the **ip pim static-rp <group> <mask> <rp>** command.

Variable	Value
<group>	Specifies the IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles.
<mask>	Specifies the address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles.
<rp>	Specifies the IP address of the static RP.

Command mode

Global configuration mode

no ip pim static-rp

Use this command to remove a static RP.

Syntax

no ip pim static-rp <group> <mask> <rp>

Variable definitions

Use the following table to help you use the **no ip pim static-rp <group> <mask> <rp>** command.

Variable	Value
<group>	Specifies the IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles.
<mask>	Specifies the address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles.
<rp>	Specifies the IP address of the static RP.

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 14: Quality of Service commands

This chapter describes ACLI Quality of Service (Qos) commands and their parameters.

For more information about QoS, see *Avaya Ethernet Routing Switch 8300 Configuration — QoS and Filter using the ACLI (NN46200-501)*.

Navigation

- interface FastEthernet/GigabitEthernet on page 392
- qos on page 392
- qos 8021p-override on page 393
- no qos 8021p-override on page 393
- qos shaper on page 394
- qos shaper rate on page 394
- qos shaper burst size on page 394
- no qos shaper on page 395
- qos trust-dscp enable on page 395
- no qos trust-dscp enable on page 395
- qos update-dynamic-mac-qos-level on page 396
- no qos update-dynamic-mac-qos-level on page 396
- qos map on page 396
- qos policy create on page 398
- no qos policy on page 399
- qos policy action on page 399
- qos policy modify on page 401
- qos egress-counter-set on page 402
- no qos egress-counter-set on page 403
- qos map-qos-level-override on page 403

interface FastEthernet/GigabitEthernet

Use this command to enter the interface configuration mode for Fast Ethernet interfaces.

Syntax

`interface FastEthernet` <*ports*> **`interface GigabitEthernet`** <*ports*>

Variable definitions

Use the following table to help you use the **`interface FastEthernet`** <*ports*> **`interface GigabitEthernet`** <*ports*> command.

Variable	Value
<*ports*>	Specifies the applicable ports associated with FastEthernet interfaces in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Global configuration mode

qos

Use this command to configure the QoS level on a port. The default is level 1, and level 7 is reserved for network traffic.

Syntax

`qos`

Variable definitions

The following table describes variables that you enter after the **`qos`** command.

Variable	Value
port <*ports*>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
8021p-override	Enables the Differentiated Service IEEE 802.1P override feature.
qos-level <*level*>	Sets the QoS level (0 to 7) associated with the traffic service class. Level 7 is reserved and cannot be set.
shaper [rate <value>] [burst-size <value>]	Enables or disables shaper on the port.

Comments? infodev@avaya.com

Variable	Value
	[rate <*value*>] sets the shaping rate in Mbps. • The actual shaping rate might be different from the configured rate due to the rate granularity of the shaper. The range is from 1 to 10000Mbps and the default is 10 • The actual burst size might be different from the configured size due to the granularity of the shaper. The range is from 4 to 16000KB, and the default is 4
trust-dscp enable	Enables or disables DSCP being trusted in an IPv4/6 packet. When enabled the dscp-to-cos-map will be used to decide on packet's traffic class and 802.1p value. This allows applications to activate Layer-3 based CoS on trusted interface. Default is disabled. **Important:** Trust DSCP can only be enabled on either 8348GTX or 8348GTX-PWR modules when in the GigabitEthenet level of ACLI
update-dynamic-mac-qos-level	Enables or disable updating of the the qos level. The default is disable.

Command mode

Interface configuration mode

qos 8021p-override

Use this command to enable the Differentiated Service IEEE 802.1P override feature.

Syntax

`qos 8021p-override`

Command mode

Interface configuration mode

no qos 8021p-override

Use this command to disable the Differentiated Service IEEE 802.1P override feature.

Syntax

no qos 8021p-override

Command mode

Interface configuration mode

qos shaper

Use this command to enable the shaper configured on a port.

Syntax

qos shaper

Command mode

Interface configuration mode

qos shaper rate

Use this command to set the shaper rate

Syntax

qos shaper rate <1-10000>

Command mode

Interface configuration mode

qos shaper burst size

Use this command to set the shaper burst size

Syntax

qos shaper burst-size <4-16000>

Command mode

Interface configuration mode

no qos shaper

Use this command to disable the shaper configured on a port.

Syntax

no qos shaper

Command mode

Interface configuration mode

qos trust-dscp enable

Use this command to enable DSCP being trusted in an IPv4/6 packet.

- Trust DSCP can only be enabled on either 8348GTX or 8348GTX-PWR modules when in the GigabitEthenet level of ACLI
- Trust DSCP should be enabled on the filter associated with the same port for consistent trust dscp operation.

Syntax

qos trust-dscp enable

Command mode

Interface GigabitEthernet configuration mode

no qos trust-dscp enable

Use this command to disable DSCP being trusted in an IPv4/6 packet.

Syntax

no qos trust-dscp enable

Command mode

Interface GigabitEthernet configuration mode

qos update-dynamic-mac-qos-level

Use this command to enable the MAC QoS level and override the port's QoS level.

Syntax

qos update-dynamic-mac-qos-level

Command mode

Interface configuration mode

no qos update-dynamic-mac-qos-level

Use this command to disable the MAC QoS level and override the port's QoS level.

Syntax

no qos update-dynamic-mac-qos-level

Command mode

Interface configuration mode

qos map

Use this command to configure QoS mapping tables.

Syntax

qos map [8021p-to-class-map <*802.1p*> <*traffic-class*> **] [8021p-to-drop-precedence-map** <*802.1p*> <*drop-precedence*> **] [class-to-8021p-map** <*traffic-class*> <*802.1p*> **] [class-to-8021p-policed-map** <*conformance-level*> <*dscp*> <*traffic-class*> <*8021p*> **] [dscp-to-cos-policed-map** <*conformance-level*> <*dscp*> <*traffic-class*> <*8021p*> <*drop-precedence*> **]**

Variable definitions

Use the following table to help you use the **qos map [8021p-to-class-map** <*802.1p*> <*traffic-class*> **] [8021p-to-drop-precedence-map** <*802.1p*> <*drop-precedence*> **] [class-to-8021p-map** <*traffic-class*> <*802.1p*> **] [class-to-8021p-policed-map** <*conformance-level*> <*dscp*> <*traffic-class*> <*8021p*> **] [dscp-to-cos-policed-map** <*conformance-level*> <*dscp*> <*traffic-class*> <*8021p*> <*drop-precedence*> **]** command.

Comments? infodev@avaya.com

Variable	Value
8021p-to-class-map <*802.1p*> <*traffic-class*>	Maps the value of the IEEE802.1 p bit (0 to 7) of the incoming packet to one of the traffic classes (0 to 7).
8021p-to-drop- precedence-map <*802.1p*> <*drop-precedence*>	Maps the value of the IEEE802.1 p bit (0 to 7) of the incoming packet to one of the following levels: • low • medium • high Packets marked with a higher drop precedence will be dropped first during periods of congestion.
class-to-8021p-map <*traffic-class*> <*802.1p*>	Maps the value of the traffic class (0 to 7) to the IEEE802.1 p bit (0 to 7) of the incoming packet.
class-to-8021p-policed-map <*conformance-level*> <*traffic-class*> <*802.1p*>	Maps the value of the traffic class (0 to 7) to the IEEE802.1 p bit (0 to 7) of the incoming packet based on one of the following conformance levels. • red means the packet exceeds the PIR (Peak Information Rate). • yellow means the packet does not exceed the PIR, but it does exceed the CIR (Committed Information Rate). • green means the packet does not exceed the CIR. The conformance level is the outcome of policing and indicates the behavior of a traffic flow.
dscp-to-cos-policed-map <*conformance-level*> <*dscp*> <*traffic-class*> <*8021p*> <*drop-precedence*>	Maps the value of the DSCP (0 to 63) to the CoS of the incoming packet based on one of the following conformance levels. • red means the packet exceeds the PIR (Peak Information Rate). • yellow means the packet does not exceed the PIR, but it does exceed the CIR (Committed Information Rate). • green means the packet does not exceed the CIR. DSCP has the following options: cs0, af11, af12, af13, cs3, c4.

Variable	Value
	The conformance level is the outcome of policing and indicates the behavior of a traffic flow. After the conformance level, enter the p bit value (0 to 7), the traffic class value (0 to 7), and the drop precedence level (low | medium | high).

Command mode

Global configuration mode

qos policy create

Use this command to create a Quality of Service policy.

Syntax

qos policy <*policy-id*> **create [<enable|disable>] [name** <*value*> **] [cir** <*value*> **] [cbs** <*value*> **] [pir** <*value*> **] [pbs** <*value*> **]**

Variable definitions

Use the following table to help you use the **qos policy** <*policy-id*> **create [<enable|disable>] [name** <*value*> **] [cir** <*value*> **] [cbs** <*value*> **] [pir** <*value*> **] [pbs** <*value*> **]** command.

Variable	Value
<*policy-id*>	Specifies the QoS policy ID number and is a unique ID in the range from 1 to 128.
<enable|disable>	Enables or disables the policy you just created. The default is disable.
name <*value*>	Names the policy. You can use up to 33 characters to identify the policy. The range is 0 to 32. If you do not assign a name, the switch automatically assigns one.
cir <*value*>	Sets the Committed Information Rate (CIR) in Kbps. The CIR is used to measure against a traffic stream. The CIR specifies the rate at which incoming traffic is measured against to be considered at a high level of conformance. The range is from 64 to 10000000, and the default is 1000.

Comments? infodev@avaya.com

Variable	Value
cbs <*value*>	Sets the Committed Burst Size (CBS) in Kbps. The CBS is used to measure against a traffic stream. The CBS specifies the maximum burst size that is supported for flows to be considered to be at a high level of conformance. The range is from 2 to 512000, and the default is 200.
pir <*value*>	Sets the Peak Information Rate (PIR) in Kbps. The PIR is used to measure against a traffic stream. The PIR specifies the rate at which incoming traffic can arrive to be considered at a medium level of conformance. The range is from 64 to 10000000, and the default is 1000.
pbs <*value*>	Sets the Peak Burst Size (PBS) in Kbps. The PBS is used to measure against a traffic stream. The PBS specifies the maximum burst size that is supported for flows to be considered to be at a medium level of conformance. The range is from 2 to 512000, and the default is 200.

Command mode

Global configuration mode

no qos policy

Use this command to delete a Quality of Service policy.

Syntax

`no qos policy` <*policy-id*>

Command mode

Interface configuration mode

qos policy action

Use this command to configure an existing Quality of Service policy.

Syntax

qos policy <*policy-id*> **action [drop rmk-cos] [rmk-8021p] [rmk-dp]**

Variable definitions

Use the following table to help you use the **qos policy** <*policy-id*> **action [drop rmk-cos] [rmk-8021p] [rmk-dp]** command.

Variable	Value
drop	Configures the policy to drop non-conforming traffic.
rmk-cos	Configures the policy to re-mark CoS parameters. The CoS parameters are re-marked according to the DSCP to CoS mapping table.
rmk-8021p	Configures the policy to re-mark the 802.1 user priority parameters. The user priority is re-marked according to the TrafficClass to 8021p mapping table.
rmk-dp	Configures the policy to re-mark drop precedence according to the conformance level.

Command mode

Global configuration mode

no qos policy action

Use this command to delete a Quality of Service policy.

Syntax

no qos policy <policy-id>action [drop] [rmk-cos] [rmk-8021p] [rmk-dp]

Variable definitions

Use the following table to help you use the **no qos policy <policy-id>action [drop] [rmk-cos] [rmk-8021p] [rmk-dp]** command.

Variable	Value
drop	Configures the policy to drop non-conforming traffic.
rmk-cos	Configures the policy to re-mark CoS parameters. The CoS parameters are re-

Variable	Value
	marked according to the DSCP to CoS mapping table.
rmk-8021p	Configures the policy to re-mark the 802.1 user priority parameters. The user priority is re-marked according to the TrafficClass to 8021p mapping table.
rmk-dp	Configures the policy to re-mark drop precedence according to the conformance level.

Command mode

Interface configuration mode

qos policy modify

Use this command to configure an existing Quality of Service policy.

Syntax

`qos policy <policy-id> modify [name` <*value*> **`] [cir`** <*value*> **`] [cbs`** <*value*> **`] [pir`** <*value*> **`] [pbs`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`qos policy <policy-id> modify [name`** <*value*> **`] [cir`** <*value*> **`] [cbs`** <*value*> **`] [pir`** <*value*> **`] [pbs`** <*value*> **`]`** command.

Variable	Value
name <*value*>	Changes the name of the policy. The range is 0 to 32 characters to identify the policy.
cir <*value*>	Changes the Committed Information Rate (CIR) in Kbps. The range is from 64 to 10000000, and the default is 1000.
cbs <*value*>	Changes the Committed Burst Size (CBS) in Kbps. The range is from 2 to 512000, and the default is 200.
pir <*value*>	Changes the Peak Information Rate (PIR) in Kbps. The range is from 64 to 10000000, and the default is 1000.
pbs <*value*>	Changes the Peak Burst Size (PBS) in Kbps. The range is from 2 to 512000, and the default is 2.

Command mode

Global configuration mode

qos egress-counter-set

Use this command to configure an egress counter that displays the statistics you want to monitor.

Syntax

qos egress-counter-set <*counter_set_id*> **[port** <*port_num*> **] [vlan** <*vlan_id*> **] [queue** <*vlan_id*> **] [dp** <*dp_level*> **]**

Variable definitions

Use the following table to help you use the **qos egress-counter-set** <*counter_set_id*> **[port** <*port_num*> **] [vlan** <*vlan_id*> **] [queue** <*vlan_id*> **] [dp** <*dp_level*> **]** command.

Variable	Value
<*counter_set_id*>	Specifies a value in the range from 1 to 40.
port <*port_num*>	Configures the port(s) that you want the counter set to monitor. If you configure one or more ports, the switch disables MONITOR ALL PORTS, which is enabled by default.
vlan <*vlan_id*>	Configures the VLAN that you want the counter set to monitor. If you configure a VLAN, the switch disables MONITOR ALL VLANS, which is enabled by default.
queue <*vlan_id*>	Configures the tx queue ID (0 to 7) that you want the counter set to monitor. If you configure a queue, the switch disables MONITOR ALL Qs, which is enabled by default.
dp <*dp_level*>	Configures the Drop Precedence level (low, medium or high) that you want the counter set to monitor. If you configure a Drop Precedence level, the switch disables MONITOR ALL DPs, which is enabled by default.

Command mode

Global configuration mode

Comments? infodev@avaya.com

no qos egress-counter-set

Use this command to delete an egress counter set.

Syntax

no qos egress-counter-set <*counter_set_id*>

Command mode

Interface configuration mode

qos map-qos-level-override

Use this command to map the MAC QoS-level override setting.

Syntax

qos map-qos-level-override

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 15: Web server commands

This chapter describes ACLI web server commands and their parameters.

Navigation

- web-server on page 405
- web-server password on page 406
- no web-server on page 406

web-server

Use this command to enable and manage or disable the Web server interface.

Syntax

`web-server [def-display-rows` <*integer*> **`] [help-tftp`** <*filename*> **`] [http-port`** <*integer*> **`]`**

Variable definitions

Use the following table to help you use the **`web-server [def-display-rows`** <*integer*> **`] [help-tftp`** <*filename*> **`] [http-port`** <*integer*> **`]`** command.

Variable	Value
[def-display-rows <*integer*>]	Specifies the number of rows displayed per page. The range of values is 10 to 100.
[help-tftp <*filename*>]	Specifies the file name, location, and path for the Web server HTML Help file. The target can be flash, pcmcia, or a TFTP IP address. The range of values is a string of 0 to 256 characters.
[http-port <*integer*>]	Specifies the http port of the Web server. The range of values is 1 to 49151.

Command mode

Global configuration mode

web-server password

Use this command to specify passwords for access to the Web server interface.

Syntax

`web-server password <ro>` <*username*> <*passwd*>

Variable definitions

Use the following table to help you use the **`web-server password <ro>`** <*username*> <*passwd*> command.

Variable	Value
<ro>	Specifies a read-only access level to the Web server interface.
<username>	Specifies the user's login name. The range of values is a string up to 20 characters. The default is ro.
<passwd>	Specifies the password associated with <*username*>. The range of values is a string up to 20 characters. The default is ro.

Command mode

Global configuration mode

no web-server

Use this command to turn off Web access.

Syntax

`no web-server`

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

Chapter 16: PoE commands

This chapter describes ACLI POE commands and their parameters.

Navigation

- poe notification slot on page 410
- no poe notification on page 411
- poe port admin on page 411
- poe priority on page 411
- poe priority in interface mode on page 412
- poe priority in global config mode on page 412
- no poe shutdown in interface GigabitEthernet mode on page 414
- poe shutdown on page 413
- no poe shutdown on page 413
- poe type on page 414
- poe usage-threshold on page 415

interface FastEthernet/GigabitEthernet

Use this command to enter the interface configuration mode for the Fast Ethernet/Gigabit Ethernet interfaces

Syntax

`interface FastEthernet/GigabitEthernet <ports>`

Variable definitions

Use the following table to help you use the **`interface FastEthernet/GigabitEthernet <ports>`** command.

Variable	Value
<*ports*>	specifies the applicable ports associated with FastEthernet interfaces in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Global configuration mode

interface FastEthernet

Use this command to enter into the interface configuration mode for Fast Ethernet interfaces.

Syntax

`interface FastEthernet` <*ports*>

Variable definitions

Use the following table to help you use the **`interface FastEthernet <ports>`** command.

Variable	Value
<*ports*>	specifies the applicable ports associated with FastEthernet interfaces in port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Global configuration mode

poe detect-control

Use this command to specify detect control for Power over Ethernet ports.

Syntax

`poe detect-control [port` <*ports*> **`] <auto|test>`**

Variable definitions

Use the following table to help you use the **`poe detect-control [port`** <*ports*> **`] <auto|test>`** command.

Comments? infodev@avaya.com

Variable	Value
[ports <*ports*>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
auto|test	Specifies automatic or test detection.

Command mode

Interface configuration mode

poe detection-control

Use this command to configure power detection control for the Power over Ethernet ports.

Syntax

`poe detection-control`

Variable definitions

The following table describes variables you enter after the **`poe detection-control`** command.

Variable	Value
[ports <*ports*>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
auto|test	Specifies automatic or test detection.

Command mode

Interface GigabitEthernet mode

poe fw-upgrade slot

Use this command to perform a firmware upgrade for a PoE card in a slot.

Syntax

`poe fw-upgrade slot` <*slots*>

Command mode

Global configuration mode

poe limit

Use this command to configure the power limit for the Power over Ethernet ports.

Syntax

poe limit [port <ports>] <3..16>

Variable definitions

This command includes the following parameters:

poe limit [port <ports>] <3..16> followed by:	
[ports <*ports*>]	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*.
<3-16>	The value to set for the port PoE power limit.

Command mode

Interface GigabitEthernet mode

poe limit in interface mode

Use this command to set the power limit for Power over Ethernet ports.

Syntax

poe limit <3-16> [port <*ports*> **]**

Command mode

Interface configuration mode

poe notification slot

Use this command to set the notification control for Power over Ethernet.

Syntax

poe notification [slot <*slots*> **]**

Command mode

Global configuration mode

no poe notification

Use this command to turn off notification control.

Syntax

no poe notification [slot <*slots*> **]**

Command mode

Global configuration mode

poe port admin

Use this command to configure the admin for the Power over Ethernet ports.

Syntax

poe port <ports> admin <enable|disable>

Variable definitions

Use the following table to help you use the **poe port <ports> admin <enable|disable>** command.

Variable	Value
<enable|disable>	Enables or disables the ports.
<ports>	Specifies the ports to enable or disable.

Command mode

Interface GigabitEthernet mode

poe priority

Use this command to configure the power priority for the Power over Ethernet ports.

Syntax

poe priority port <ports> <low|high|critical>

Variable definitions

Use the following table to help you use the **poe priority port <ports> <low|high|critical>** command.

Variable	Value
port<ports>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*
<low|high|critical>	Specify the power priorites.

Command mode

Interface GigabitEthernet mode

poe priority in interface mode

Use this command to set port priority for Power over Ethernet.

Syntax

`poe priority [port` *<ports>* **`] <low|high|critical>`**

Variable definitions

Use the following table to help you use the **`poe priority port <ports> <low|high|critical>`** command.

Variable	Value
port<ports>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*
<low|high|critical>	Specify the power priorites.

Command mode

Interface configuration mode

poe priority in global config mode

Use this command to enable Power over Ethernet on a particular slot or slots.

Syntax

`poe priority [slot` *<slots>* **`] <low|high|critical>`**

Variable definitions

Use the following table to help you use the **`poe priority port <ports> <low|high|critical>`** command.

Variable	Value
port<ports>	Specifies the applicable ports in port list form: *{slot/port [-slot/port][, ...]}*
<low|high|critical>	Specify the power priorites.

Command mode

Global configuration mode

poe shutdown

Use this command to shut down Power over Ethernet on specified ports.

Syntax

poe shutdown [port <*ports*> **]**

Command mode

Interface configuration mode

no poe shutdown

Use this command to specify no shutdown of Power over Ethernet.

Syntax

no poe shutdown [port <*ports*> **]**

Command mode

Interface configuration mode

poe shutdown in global config mode

Use this command to disable Power over Ethernet for specified slots.

Syntax

poe shutdown slot <*slots*>

Command mode

Global configuration mode

no poe shutdown in interface GigabitEthernet mode

Use this command to specify disabling the Power over Ethernet function for specified ports.

Syntax

no poe shutdown port [port <ports>]

Variable definitions

Use the following table to help you use the **no poe shutdown port [port <ports>]** command.

Variable	Value
<portlist>	Selects the portlist {port[-port][,...]}.

Command mode

Interface GigabitEthernet mode

no poe shutdown

Use this command to specify disabling the Power over Ethernet function for specified slots.

Syntax

no poe shutdown [slot <*slots*> **]**

Command mode

Global configuration mode

poe type

Use this command to set the port type for Power over Ethernet.

Syntax

poe type [port <*ports*> **] <other|telephone|webcam|wireless>**

Variable definitions

Use the following table to help you use the **poe type [port** <*ports*> **] <other|telephone|webcam|wireless>** command.

Comments? infodev@avaya.com

Variable	Value
port <*ports*>	Specifies ports as the poe port type.
other	Specifies another device as the poe port type.
telephone	Specifies a telephone poe port type.
webcam	Specifies webcam as the poe port type.
wireless	Specifies wireless as the poe port type.

poe type port

Use this command to configure the type of Power over Ethernet ports.

Syntax

`poe type port <ports> <other|telephone|webcam|wireless>`

Variable definitions

The following table describes variables that help you enter after the **`poe type port <ports>`** command.

Variable	Value
other	Specifies another device as the poe port type.
telephone	Specifies a telephone poe port type.
webcam	Specifies webcam as the poe port type.
wireless	Specifies wireless as the poe port type.

Command mode

Interface configuration mode

poe usage-threshold

Use this command to set the usage threshold for Power over Ethernet for a particular slot or slots.

Syntax

`poe usage-threshold [slot` <*slots*> **`]`**

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 17: LACP commands

This chapter describes ACLI LACP and VLACP commands and their parameters.

Navigation

- lacp on page 417
- no lacp on page 419
- show lacp interface on page 419
- lacp on port on page 420
- no lacp on port on page 422
- show vlacp on page 422
- vlacp enable on page 423
- no vlacp enable on page 423
- vlacp on a port on page 425
- no vlacp enable on a port on page 426
- show vlacp interface on page 427
- lacp enable on an mlt on page 427
- no lacp on an mlt on page 428
- show mlt on page 428

lacp

Use this command to configure LACP globally.

Syntax

lacp

Variable definitions

Use the following table to help you use the **lacp** command.

Variable	Value
aggr-wait-time <milliseconds>	Sets the aggregation wait time (in milliseconds) for a specific port type. The value ranges from 200 to 2000 ms.
enable	Enables LACP globally on the switch.
fast-periodic-time <milliseconds>	Sets the fast-periodic time (in milliseconds) for a specific port type. The value ranges from 200 to 20000 ms. **Important:** If you make configuration changes to the fast periodic time value of an LAG member, you must make the same configuration changes to the fast periodic time value of all ports in the LAG and member ports of the protocol partner.
low-periodic-time <milliseconds>	Sets the slow periodic time (in milliseconds) for a specific port type. The value ranges from 10 000 to 30 000 ms. **Important:** If you make configuration changes to the slow periodic time value of an LAG member, you must make the same configuration changes to the slow periodic time value of all ports in the LAG and member ports of the protocol partner.
smlt-sys-id	Sets the LACP system ID globally.
system-priority	Sets the LACP system priority globally. The value ranges from 0 to 65 535. The default value is 32,768. **Important:** Global LACP system-priority overwrites the LACP system-priority of all LAGs and ports. You must configure LACP system-priority for LAGs or ports on a switch to the same value as the global LACP system-priority of that switch.
timeout-scale <integer>	Sets a timeout scale for a specific port type. The value ranges from 2 to 10 and the default value is 3.

Command mode

Global configuration mode

no lacp

Use this command to delete LACP globally.

Syntax

`no lacp`

Command mode

Global configuration mode

show lacp interface

Use this command to view the LACP configuration information.

Syntax

`show lacp interface`

Variable definitions

Use the following table to help you use the **`show lacp interface`** command.

Variable	Value
fastethernet <slot/port><vid>	Specifies the FastEthernet interface slot and port. <*vid*> is the VLAN id. Values range from 1 to 4000.
Gigabitethernet <slot/port><vid>	Specifies the GigabitEthernet interface slot and port. <*vid*> is the VLAN id. Values range from 1 to 4000.
mlt <64-6174>	Specifies MLT LACP information. <*64-6174*> is the Ifindex.
pos <slot/port><vid>	Shows Packet over SONET (PoS) interface LACP configuration. • <*slot/port*> is the slot and the port. • <*vid*> is the VLAN id in the range of 1 to 4000.

Command mode

Privileged EXEC mode

lacp on port

Use this command to configure LACP on a port.

Syntax

`lacp`

Variable definitions

Use the following table to help you use the **`lacp`** command.

Variable	Value
aggr-wait-time <milliseconds>	Sets the aggregation wait time (in milliseconds) for a specific port type. The value ranges from 200 to 2000 ms.
enable	Enables LACP on port.
aggregation	Enables lacp aggregation.
clear-stats	Clears lacp statistics.
fast-periodic-time <milliseconds>	Sets the fast-periodic time (in milliseconds) for a specific port type. The value ranges from 200 to 20000 ms. **Important:** If you make configuration changes to the fast periodic time value of an LAG member, you must make the same configuration changes to the fast periodic time value of all ports in the LAG and member ports of the protocol partner.
key <integer>	Sets the aggregation key for the port. The value is an integer in the range of 0 to 65535.
mode <active|passive>	Selects an active or passive mode type.
partner-key <integer>	Sets the partner administration key value. The value is an integer in the range of 0 to 65535.
partner-port <integer>	Sets the partner administration port value. The value is a number in the range of 0 to 65535.
partner-port-priority <integer>	Sets the partner administration port priority value. The value is a number in the range of 0 to 65535.

Variable	Value
partner-state <hex>	Sets the port-partner administration state value. The hexadecimal value represents the LACP partner administrative state bitmap.
partner-system-id <mac>	Sets the port partner administration system ID. The value is the LACP partner administrative system ID MAC address.
partner-system-priority <integer>	Sets the partner administration system priority value. The value is an integer in the range of 0 to 65535.
priority <integer>	Sets the port priority value. The value is an integer in the range of 0 to 65535.
slow-periodic-time <milliseconds>	Sets the slow periodic time for a specific port type. The value ranges from 10000 to 30000 ms. **Important:** If you make configuration changes to the slow periodic time value of an LAG member, you must make the same configuration changes to the slow periodic time value of all ports in the LAG and member ports of the protocol partner.
system-priority <integer>	Sets the lacp system priority globally. The value is an integer in the range of 0 to 65535. The default value is 32,768. **Important:** Global LACP system-priority overwrites the LACP system-priority of all LAGs and ports. You must configure LACP system-priority for LAGs or ports on a switch to the same value as the global LACP system-priority of that switch.
timeout-scale <integer>	Sets a timeout scale for a specific port type. The value ranges from 1 to 10. The default value is 3.
timeout-time <long|short>	Sets the timeout value to either long or short for a specific port type.

Command mode

FastEthernet or GigabitEthernet Interface Configuration

no lacp on port

Use this command to delete LACP on a port.

Syntax

no lacp

Command mode

FastEthernet or GigabitEthernet Interface Configuration

show vlacp

Use this command to view LACP configuration information to review and confirm the configuration of LACP parameters, globally or for a specific interface.

Syntax

show vlacp

Command mode

FastEthernet or GigabitEthernet configuration mode

Variable definitions

The following table describes optional parameters that you enter after the **show vlacp** command.

Variable	Value
actor-admin interface<fastethernet|gigabitethernet>	Displays the port lacp actor administrative information.
actor-oper interface<fastethernet|gigabitethernet>	Displays the port lacp actor operational information.
extension interface<fastethernet|gigabitethernet>	Displays the port lacp timer information.
interface<fastethernet|gigabitethernet>	Displays the lacp interface information.
partner-admin interfacefastethernet|gigabitethernet>	Displays the port lacp partner administrative information.
partnet-oper<fastethernet|gigabitethernet>	Displays the port lacp partner operational information.

vlacp enable

Use this command to enable VLACP globally.

Syntax

`vlacp enable`

Command mode

Global Configuration mode

default vlacp enable

Use this command to configure VLACP to the switch default (disable).

Syntax

`default vlacp enable`

Command mode

Global configuration mode

no vlacp enable

Use this command to disable VLACP globally.

Syntax

`no vlacp enable`

Command mode

Global Configuration mode

vlacp macaddress

Use this command to configure the default multicast MAC address the switch uses for VLACP PDUs.

Important:
You can only configure the VLACP MAC address when VLACP is disabled globally.

Syntax

`vlacp macaddress <macaddress>`

Variable definitions

Use the following table to help you use the **`vlacp macaddress <macaddress>`** command.

Variable	Value
<macaddress>	Specifies a MAC address ranging from 01:80:c2:00:00:00 to 01:80:c2:00:ff:ff. You cannot use the following MAC addresses for VLACP PDUs: • 01:80:c2:00:00:00—reserved for BPDU • 01:80:c2:00:00:21—reserved for gvrp • 01:80:c2:00:00:0e—reserved for SLPP • 01:80:c2:00:00:02—reserved for LACP • 01:80:c2:00:00:03—reserved for EAP • 01:80:c2:00:00:01—reserved for the flow control terminal

Command mode

Global Configuration mode

default vlacp macaddress

Use this command to configure the multicast MAC address to the default value.

Syntax

`default vlacp macaddress`

Command mode

Global configuration mode

no vlacp macaddress

Use this command to discontinue using a default multicast MAC address for the switch to use for VLACP PDUs.

Important:

You can only configure the VLACP MAC address when VLACP is disabled globally.

Syntax

`no vlacp macaddress`

Command mode

Global Configuration mode

vlacp on a port

Use this command to configure VLACP on a port.

Syntax

`vlacp`

Variable definitions

Use the following table to help you use the **`vlacp`** command.

Variable	Value
enable	Enables VLACP on the port.
ethertype	Specifies the VLACP protocol identification. The value is a hexadecimal number ranging from 0x5f3 to 0xffff.
fast-periodic-time <milliseconds>	Sets the fast-periodic time (in milliseconds) for a specific port type. The value ranges from 200 to 20000 ms.
low-slow periodic-time <milliseconds>	Sets the slow periodic time (in milliseconds) for a specific port type. The value ranges from 10 000 to 30 000 ms.
timeout <slow|long>	Sets the timeout as long or slow.
timeout-scale <integer>	Sets a timeout scale for a specific port type. The value ranges from 2 to 10 and the default value is 3.

Command mode

Interface Configuration mode

default vlacp on a port

Use this command to configure VLACP on a port to default values.

Syntax

`default vlacp`

Variable definitions

Use the following table to help you use the **`default vlacp`** command.

Variable	Value
enable	Disables VLACP on the port.
ethertype	Configures the VLACP protocol identification to default (0x8103).
fast-periodic-time	Configures the fast-periodic time (in milliseconds) for a specific port type to default.
slow-periodic-time	Configures the slow periodic time (in milliseconds) for a specific port type to default.
timeout	Configures the timeout to default.
timeout-scale	Configures the timeout scale for a specific port type to default. The default value is 3.

Command mode

Interface configuration mode

no vlacp enable on a port

Use this command to disable VLACP on a port.

Syntax

`no vlacp enable`

Command mode

Interface Configuration mode

Comments? infodev@avaya.com

show vlacp interface

Use this command to view port specific VLACP configuration information.

Syntax

`show vlacp interface`

Command mode

Global configuration mode

Variable definitions

The following table describes optional parameters that you enter after the **`show vlacp interface`** command.

Variable	Value
fastethernet	Specifies the Fastethernet port interface.
gigabitethernet	Specifies the GigabitEthernet port interface.
pos	Specifies the PoS port interface.

lacp enable on an mlt

Use this command to configure LACP on an MLT to provide dynamic link aggregation mechanisms.

Syntax

`lacp`

Variable definitions

Use the following table to help you use the **`lacp`** command.

Variable	Value
key <integer>	Sets the LACP key for a specific MLT. Integer is the LACP aggregator key with a range of 0 to 256.
enable	Enables LACP for a specific MLT.
system-priority <integer>	Sets LACP system priority for a specific MLT. Integer is the system priority with a range of 0 to 65 535.

Command mode

MLT Interface Configuration mode

no lacp on an mlt

Use this command to disable LACP on an MLT to provide dynamic link aggregation mechanisms.

Syntax

no lacp enable

Command mode

MLT Interface Configuration mode

show mlt

Use this command to view configuration information about all MLTs or a specific MLT configured on a switch.

Syntax

show mlt

Command mode

Privileged EXEC mode

Chapter 18: BGP Lite commands

This chapter describes the ACLI commands and parameters you use to configure Border Gateway Protocol (BGP).

Navigation

- aggregate-address on page 432
- default aggregate-address on page 433
- no aggregate-address on page 434
- auto-peer-restart enable on page 435
- default auto-peer-restart enable on page 435
- no auto-peer-restart enable on page 435
- auto-summary on page 436
- default auto-summary on page 436
- no auto-summary on page 436
- bgp aggregation enable on page 436
- default bgp aggregation enable on page 437
- no bgp aggregation enable on page 437
- bgp client-to-client reflection on page 437
- default bgp client-to-client reflection on page 438
- no bgp client-to-client reflection on page 438
- bgp cluster-id on page 438
- no bgp cluster-id on page 439
- bgp default local-preference on page 439
- default bgp default local-preference on page 440
- no bgp default local-preference on page 440
- bgp multiple-paths on page 440
- default bgp multiple-paths on page 441

- debug-screen on page 441
- default debug-screen on page 441
- no debug-screen on page 442
- default-information originate on page 442
- default default-information originate on page 442
- no default-information originate on page 442
- global-debug mask on page 443
- default global-debug mask on page 444
- no global-debug mask on page 444
- ibgp-report-import-rt enable on page 444
- default ibgp-report-import-rt enable on page 445
- no ibgp-report-import-rt enable on page 445
- ignore-illegal-rtrid enable on page 445
- default ignore-illegal-rtrid enable on page 446
- no ignore-illegal-rtrid enable on page 446
- neighbor on page 446
- default neighbor on page 449
- no neighbor on page 451
- neighbor-debug-all mask on page 453
- network on page 454
- default network on page 455
- no network on page 455
- no-med-path-is-worst enable on page 456
- default no-med-path-is-worst enable on page 456
- no no-med-path-is-worst enable on page 456
- quick-start enable on page 456
- default quick-start enable on page 457
- no quick-start enable on page 457
- redistribute on page 457
- default redistribute on page 458
- no redistribute on page 458
- route-reflector enable on page 459

- default route-reflector enable on page 459
- no route-reflector enable on page 460
- route-refresh on page 460
- default route-refresh on page 460
- no route-refresh on page 460
- router-id on page 461
- no router-id on page 461
- synchronization on page 461
- default synchronization on page 462
- no synchronization on page 462
- traps enable on page 462
- default traps enable on page 462
- no traps enable on page 463
- router bgp on page 463
- no router bgp enable on page 463
- neighbor on page 464
- no neighbor on page 467
- default neighbor on page 469
- neighbor password on page 470
- no neighbor password on page 471
- default neighbor password on page 471
- redistribute on page 472
- default redistribute on page 473
- ip bgp apply redistribute on page 473
- no redistribute on page 473
- ip as-list on page 474
- no ip as-list on page 475
- ip community-list on page 475
- no ip community-list on page 476
- ip bgp restart-bgp on page 477
- ip bgp stats-clear-counters on page 477
- ip bgp stats-clear-counters neighbor on page 478

- show ip bgp aggregates on page 478
- show ip bgp cidr-only on page 478
- show ip bgp conf on page 479
- show ip bgp neighbors on page 479
- show ip bgp networks on page 480
- show ip bgp peer-group on page 480
- show ip bgp route on page 481
- show ip bgp redistributed-routes on page 481
- show ip bgp summary on page 482
- show ip bgp stats on page 482

aggregate-address

Use this command to add an aggregate address to a BGP routing table.

Syntax

aggregate-address <a.b.c.d/len> [advertise-map <WORD 0-1536>] [as-set] [attribute-map <WORD 0-1536>] [summary-only] [suppress-map <WORD 0-1536>]

Variable definitions

Use the following table to help you use the **aggregate-address <a.b.c.d/len> [advertise-map <WORD 0-1536>] [as-set] [attribute-map <WORD 0-1536>] [summary-only] [suppress-map <WORD 0-1536>]** command.

Variable	Value
<a.b.c.d/len>	Is an IP address and an integer value (between 0 and 32)
advertise-map <WORD 0-1536>	Is the route map name (any string length between 0 and 64 characters long) for route advertisements.
as-set	Enables autonomous system information. The default value is disable.
attribute-map <WORD 0-1536>	Is the route map name (string length between 0 and 64 characters long).
summary-only	Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses

Variable	Value
	advertisements of more specific routes to all neighbors. The default value is disable.
suppress-map <WORD 0-1536>	Is the route map name (string length between 0 and 64 characters long) for the suppressed route list.

Command mode

BGP configuration mode

default aggregate-address

Use this command to configure aggregate address information in the BGP routing table to default values.

Syntax

`default aggregate-address <a.b.c.d/len> [advertise-map <WORD 0-1536>] [as-set] [attribute-map <WORD 0-1536>] [summary-only] [suppress-map <WORD 0-1536>]`

Variable definitions

Use the following table to help you use the **`default aggregate-address <a.b.c.d/len> [advertise-map <WORD 0-1536>] [as-set] [attribute-map <WORD 0-1536>] [summary-only] [suppress-map <WORD 0-1536>]`** command.

Variable	Value
<a.b.c.d/len>	Is an IP address and an integer value (between 0 and 32)
advertise-map <WORD 0-1536>	Is the route map name (any string length between 0 and 64 characters long) for route advertisements.
as-set	Enables autonomous system information. The default value is disable.
attribute-map <WORD 0-1536>	Is the route map name (string length between 0 and 64 characters long).
summary-only	Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.

Variable	Value
suppress-map <WORD 0-1536>	Is the route map name (string length between 0 and 64 characters long) for the suppressed route list.

Command mode

BGP configuration mode

no aggregate-address

Use this command to delete an aggregate address from a BGP routing table.

Syntax

no aggregate-address <a.b.c.d/len> [advertise-map <WORD 0-1536>] [as-set] [attribute-map <WORD 0-1536>] [summary-only] [suppress-map <WORD 0-1536>]

Variable definitions

Use the following table to help you use the **no aggregate-address <a.b.c.d/len> [advertise-map <WORD 0-1536>] [as-set] [attribute-map <WORD 0-1536>] [summary-only] [suppress-map <WORD 0-1536>]** command.

Variable	Value
<a.b.c.d/len>	Is an IP address and an integer value (between 0 and 32)
advertise-map <WORD 0-1536>	Is the route map name (any string length between 0 and 64 characters long) for route advertisements.
as-set	Disables autonomous system information. The default value is disable.
attribute-map <WORD 0-1536>	Is the route map name (string length between 0 and 64 characters long).
summary-only	Disables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.
suppress-map <WORD 0-1536>	Is the route map name (string length between 0 and 64 characters long) for the suppressed route list.

Comments? infodev@avaya.com

Command mode

BGP configuration mode

auto-peer-restart enable

Use this command to enable the process that automatically restarts a connection to a BGP neighbor.o.

Syntax

auto-peer-restart enable

Command mode

BGP configuration mode

default auto-peer-restart enable

Use this command to enable the process that automatically restarts a connection to a BGP neighbor.

Syntax

default auto-peer-restart enable

Command mode

BGP configuration mode

no auto-peer-restart enable

Use this command to disable the process that automatically restarts a connection to a BGP neighbor.o.

Syntax

auto-peer-restart enable

Command mode

BGP configuration mode

auto-summary

Use this command to enable BGP to summarize networks based on class limits.

Syntax

`auto-summary`

Command mode

BGP configuration mode

default auto-summary

Use this command to enable BGP to summarize networks based on class limits.

Syntax

`default auto-summary`

Command mode

BGP configuration mode

no auto-summary

Use this command to disable BGP to summarize networks based on class limits.

Syntax

`auto-summary`

Command mode

BGP configuration mode

bgp aggregation enable

Use this command to enable the aggregation feature on this interface. You cannot change the value when BGP is enabled.

Syntax

bgp aggregation enable

Command mode

BGP configuration mode

default bgp aggregation enable

Use this command to enable the aggregation feature on this interface. You cannot change the value when BGP is enabled.

Syntax

default bgp aggregation enable

Command mode

BGP configuration mode

no bgp aggregation enable

Use this command to disable the aggregation feature on this interface. You cannot change the value when BGP is enabled.

Syntax

no bgp aggregation enable

Command mode

BGP configuration mode

bgp client-to-client reflection

Use this command to enable route reflection between two route reflector clients.

Syntax

bgp client-to-client reflection

Command mode

BGP configuration mode

default bgp client-to-client reflection

Use this command to enable route reflection between two route reflector clients.

Syntax

`default bgp client-to-client reflection`

Command mode

BGP configuration mode

no bgp client-to-client reflection

Use this command to disable route reflection between two route reflector clients.

Syntax

`no bgp client-to-client reflection`

Command mode

BGP configuration mode

bgp cluster-id

Use this command to configure a cluster ID.

Syntax

`bgp cluster-id <A.B.C.D>`

Variable definitions

Use the following table to help you use the **`bgp cluster-id <A.B.C.D>`** command.

Variable	Value
<A.B.C.D>	Specifies the cluster ID of the reflector router.

Command mode

BGP configuration mode

no bgp cluster-id

Use this command to disable a cluster ID.

Syntax

no bgp cluster-id <A.B.C.D>

Variable definitions

Use the following table to help you use the **no bgp cluster-id <A.B.C.D>** command.

Variable	Value
<A.B.C.D>	Specifies the cluster ID of the reflector router.

Command mode

BGP configuration mode

bgp default local-preference

Use this command to configure the default local preference attribute.

Syntax

bgp default local-preference <0-2147483647>

Variable definitions

Use the following table to help you use the **bgp default local-preference <0-2147483647>** command.

Variable	Value
<0-2147483647>	Specifies the default local preference range. The default is 0.

Command mode

BGP configuration mode

default bgp default local-preference

Use this command to configure the default local preference attribute to the default value.

Syntax

`default bgp default local-preference`

Command mode

BGP configuration mode

no bgp default local-preference

Use this command to disable the default local preference attribute.

Syntax

`no bgp default local-preference <0-2147483647>`

Variable definitions

Use the following table to help you use the **`no bgp default local-preference <0-2147483647>`** command.

Variable	Value
<0-2147483647>	Specifies the default local preference range. The default is 0.

Command mode

BGP configuration mode

bgp multiple-paths

Use this command to configure the maximum number of equal-cost-paths that are available to a BGP router.

Syntax

`bgp multiple-paths <1-4>`

Variable definitions

Use the following table to help you use the **`bgp multiple-paths <1-4>`** command.

Variable	Value
<1-4>	Specifies the maximum number of equal cost routes. The default value is 1.

Command mode

BGP configuration mode

default bgp multiple-paths

Use this command to configure the maximum number of equal-cost-paths that are available to a BGP router to the default value (1).

Syntax

`default bgp multiple-paths`

Command mode

BGP configuration mode

debug-screen

Use this command to disable BGP debug screen logging (off) or enable BGP screen logging (on). The default is off.

Syntax

`debug-screen <off|on>`

Command mode

BGP configuration mode

default debug-screen

Use this command to configure BGP debug screen logging to the default (off).

Syntax

`default debug-screen`

Command mode

BGP configuration mode

no debug-screen

Use this command to disable BGP debug screen logging.

Syntax

no debug-screen

Command mode

BGP configuration mode

default-information originate

Use this command to enable the advertisement of a default route to peers, if it is present in the routing table. The default value is disable.

Syntax

default-information originate

Command mode

BGP configuration mode

default default-information originate

Use this command to disable the advertisement of a default route to peers, if it is present in the routing table.

Syntax

default default-information originate

Command mode

BGP configuration mode

no default-information originate

Use this command to disable the advertisement of a default route to peers, if it is present in the routing table.

Syntax

`no default-information originate`

Command mode

BGP configuration mode

global-debug mask

Use this command to display specified debug information for BGP global configurations.

Syntax

`global-debug mask <WORD 1-100>`

Variable definitions

Use the following table to help you use the **`global-debug mask <WORD 1-100>`** command.

Variable	Value
<*WORD 1-100*>	Specifies a list of mask choices separated by commas with no space between choices. The default value is none. Mask choices are: • *none*—disables all debug messages. • *all*—enables all debug messages. • *error*—enables display of debug error messages. • *packet*—enables display of debug packet messages. • *event*—enables display of debug event messages. • *trace*—enables display of debug trace messages. • *warning*—enables display of debug warning messages. • *state*—enables display of debug state transition messages. • *init*—enables display of debug initialization messages.

Variable	Value
	• *filter*—enables display of debug messages related to filtering. • *update*—enables display of debug messages related to sending and receiving updates.

Command mode

BGP configuration mode

default global-debug mask

Use this command to configure the specified debug information display for BGP global configurations to the default (none).

Syntax

`default global-debug mask`

Command mode

BGP configuration mode

no global-debug mask

Use this command to disable the displaying of specified debug information for BGP global configurations.

Syntax

`no global-debug mask`

Command mode

BGP configuration mode

ibgp-report-import-rt enable

Use this command to configure BGP to advertise imported routes to an interior BGP (IBGP) peer. This command also enables or disables advertisement of non-BGP imported routes to other IBGP neighbors. The default value is enable..

Syntax

ibgp-report-import-rt enable

Command mode

BGP configuration mode

default ibgp-report-import-rt enable

Use this command to configure BGP to advertise imported routes to an interior BGP (IBGP) peer. This command also enables or disables advertisement of non-BGP imported routes to other IBGP neighbors.

Syntax

default ibgp-report-import-rt enable

Command mode

BGP configuration mode

no ibgp-report-import-rt enable

Use this command to disable BGP from advertising imported routes to an interior BGP (IBGP) peer.

Syntax

no ibgp-report-import-rt enable

Command mode

BGP configuration mode

ignore-illegal-rtrid enable

Use this command to enable BGP to overlook an illegal router ID. Enable is the default.

Syntax

ignore-illegal-rtrid enable

Command mode

BGP configuration mode

default ignore-illegal-rtrid enable

Use this command to enable BGP to overlook an illegal router ID.

Syntax

`default ignore-illegal-rtrid enable`

Command mode

BGP configuration mode

no ignore-illegal-rtrid enable

Use this command to disable BGP from overlooking an illegal router ID.

Syntax

`no ignore-illegal-rtrid enable`

Command mode

BGP configuration mode

neighbor

Use this command to configure peers or peer groups.

Syntax

`neighbor <PT_IPORPEERGROUP>`

Variable definitions

Use the following table to help you use the **`neighbor <PT_IPORPEERGROUP>`** command.

Variable	Value
default-originate	Enables the switch to send a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. The default value is disable. Do not use this command if `default-information originate` is globally enabled.

Comments? infodev@avaya.com

Variable	Value
enable	Enables the BGP neighbor.
in-route-map <WORD 0-256>	Applies a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates. <*WORD 0-256*> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.
max-prefix <0-2147483647>	Sets a limit on the number of routes that can be accepted from a neighbor. The default value is 12000 routes. A value of 0 (zero) indicates that there is no limit to the number of routes that can be accepted.
MD5-authentication enable	Enables TCP MD5 authentication between two peers. The default value is disable.
neighbor-debug mask <WORD 1-100>	Displays specified debug information for a BGP peer. The default value is none. <*WORD 1-100*> is a list of mask choices separated by commas with no space between choices. For example: *{<mask>,<mask>,<mask>...}*. Mask choices are: *none* disables all debug messages. *all* enables all debug messages. *error* enables display of debug error messages. *packet* enables display of debug packet messages. *event* enables display of debug event messages. *trace* enables display of debug trace messages. *warning* enables display of debug warning messages. *state* enables display of debug state transition messages. *init* enables display of debug initialization messages. *filter* enables display of debug messages related to filtering. *update* enables display of debug messages related to sending and receiving updates.

Variable	Value
next-hop-self	When enabled, specifies that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. The default value is disable. The next-hop parameter can only be configured when the neighbor is disabled.
out-route-map <WORD 0-256>	Applies a route policy rule to all outgoing routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates. <*WORD 0-256*> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.
peer-group <WORD 0-1536>	Adds a BGP peer to the specified subscriber group. You must create the specified subscriber group before you issue this command.
<PT_IPORPEERGROUP>	Specifies the peer IP address or the peer group name.
remote-as <0-65535>	Configures the remote AS number of a BGP peer or a peer-group. You cannot configure this option when the admin-state is enable.
retry-interval <1-65535>	Sets the time interval (in seconds) for the ConnectRetry Timer. The default value is 120 seconds.
route-reflector-client	Configures the specified neighbor or group of neighbors as its route reflector client. The default value is disable. All neighbors that are configured become members of the client group and the remaining IBGP peers become members of the nonclient group for the local route reflector.
route-refresh	Enables route refresh for the BGP peer. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.

Variable	Value
send-community	Enables the switch to send the update message community attribute to the specified peer. The default value is disable.
soft-reconfiguration-in enable	When enabled, the router relearns routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable.
timers <0-21845>	Configures timers (in seconds) for the BGP speaker for this peer. <*0-21845*> is the keep alive time.
update-source <A.B.C.D>	Specifies the source IP address when BGP packets are sent to this peer or peer group. You cannot configure this parameter when the admin-state is enable. <*A.B.C.D*> is the specified source IP address.
weight <0-65535	Specifies the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer. The default value is 0. If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor.

Command mode

BGP configuration mode

default neighbor

Use this command to configure specific BGP neighbor parameters to default values.

Syntax

`default neighbor <PT_IPORPEERGROUP>`

Variable definitions

Use the following table to help you use the **`default neighbor <PT_IPORPEERGROUP>`** command.

Variable	Value
default-originate	Configures the BGP neighbor default-originate parameter to the default value, disable.
enable	Configures the BGP neighbor enable parameter to default.
in-route-map	Configures the BGP neighbor in-route policy to default.
max-prefix	Configures the BGP neighbor maximum prefix to the default value, 12000 routes.
MD5-authentication enable	Configures the BGP neighbor TCP MD5 authentication to the default value, disable.
neighbor-debug-mask	Configures the BGP neighbor debug information for a BGP peer to the default value, none.
next-hop-self	Configures the BGP neighbor next-hop attribute to the default value, disable. The next-hop parameter can only be configured when the neighbor is disabled.
out-route-map	Configures the BGP neighbor outgoing route policy to the default value.
<PT_IPORPEERGROUP>	Specifies the peer IP address or the peer group name.
remote-as	Configures the BGP neighbor remote AS number of a BGP peer or a peer-group to the default value. You cannot configure this option when the admin-state is enable.
retry-interval	Configures the BGP neighbor time interval (in seconds) for the ConnectRetry Timer to the default value, 120 seconds.
route-refresh	Configures the BGP neighbor route refresh for the BGP peer to the default value.
send-community	Configures the switch to send the default update message community attribute to the specified peer. The default value is disable.
soft-reconfiguration-in enable	Configures the switch default for relearning routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable.

Variable	Value
timers	Configures the BGP neighbor keep alive and hold timers (in seconds) for the BGP speaker for this peer to the default value.
update-source	Configures the source IP address when BGP packets are sent to this peer or peer group to the default value. You cannot configure this parameter when the admin-state is enable.
weight	Configures the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer to the default value, 0.

Command mode

BGP configuration mode

no neighbor

Use this command to delete neighbors from peer groups and peer associations or to discontinue using specific BGP neighbor parameters.

Syntax

`no neighbor <PT_IPORPEERGROUP>`

Variable definitions

Use the following table to help you use the **`no neighbor <PT_IPORPEERGROUP>`** command.

Variable	Value
default-originate	Prevents the switch from sending a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. The default value is disable.
enable	Disables the BGP neighbor.
in-route-map	Discontinues the application of a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates.

Variable	Value
MD5-authentication enable	Disables TCP MD5 authentication between two peers. The default value is disable.
neighbor-debug-mask <WORD 1-100>	Discontinues displaying specified debug information for a BGP peer. <*WORD 1-100*> is a list of mask choices separated by commas with no space between choices. For example: *{<mask>,<mask>,<mask>...}*. Mask choices are: *none* disables all debug messages. *all* enables all debug messages. *error* enables display of debug error messages. *packet* enables display of debug packet messages. *event* enables display of debug event messages. *trace* enables display of debug trace messages. *warning* enables display of debug warning messages. *state* enables display of debug state transition messages. *init* enables display of debug initialization messages. *filter* enables display of debug messages related to filtering. *update* enables display of debug messages related to sending and receiving updates.
next-hop-self	Discontinues specifying that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. The default value is disable. The next-hop parameter can only be configured when the neighbor is disabled.
out-route-map	Discontinues applying a route policy rule to all outgoing routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates.
peer-group	Deletes a BGP neighbor peer group.
<PT_IPORPEERGROUP>	Specifies the peer IP address or the peer group name.

Variable	Value
remote-as	Deletes the BGP peer or a peer-group remote AS.
route-reflector-client	Disables the specified neighbor or neighbors route reflector clients. The default value is disable.
route-refresh	Disables route refresh for the BGP peer.
send-community	Disables the switch from sending the update message community attribute to the specified peer. The default value is disable.
soft-reconfiguration-in enable	When disabled, the router does not relearn routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable.
update-source	Disables specifying the source IP address when BGP packets are sent to this peer or peer group. You cannot configure this parameter when the admin-state is enable.
weight	Disables specifying the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer.

Command mode

BGP configuration mode

neighbor-debug-all mask

Use this command to display specified debug information for BGP neighbors.

Syntax

`neighbor-debug-all mask <WORD 1-100>`

Variable definitions

Use the following table to help you use the **`neighbor-debug-all mask <WORD 1-100>`** command.

Variable	Value
<*WORD 1-100*>—	Specifies a list of mask choices separated by commas with no space between choices. For example:*{<mask>,<mask>,<mask>...}*.

Variable	Value
	Mask choices are: *none*—disables all debug messages. *all*—enables all debug messages. *error*—enables display of debug error messages. *packet*—enables display of debug packet messages. *event*—enables display of debug event messages. *trace*—enables display of debug trace messages. *warning*—enables display of debug warning messages. *state*—enables display of debug state transition messages. *init*—enables display of debug initialization messages. *filter*—enables display of debug messages related to filtering. *update*—enables display of debug messages related to sending and receiving updates.

Command mode

BGP configuration mode

network

Use this command to specify IGP network prefixes for BGP to advertise for redistribution. This command imports routes into BGP.

Syntax

`network <PT_IPNLEN>`

Variable definitions

Use the following table to help you use the **`network <PT_IPNLEN>`** command.

Variable	Value
<PT_IPNLEN>	Specifies the network address and mask.

Command mode

BGP configuration mode

default network

Use this command to specify default IGP network prefixes for BGP to advertise for redistribution. This command imports routes into BGP.

Syntax

`default network <PT_IPNLEN>`

Variable definitions

Use the following table to help you use the **`default network <PT_IPNLEN>`** command.

Variable	Value
<PT_IPNLEN>	Specifies the network address and mask.

Command mode

BGP configuration mode

no network

Use this command to disable specifying IGP network prefixes for BGP to advertise for redistribution.

Syntax

`no network <PT_IPNLEN>`

Variable definitions

Use the following table to help you use the **`no network <PT_IPNLEN>`** command.

Variable	Value
<PT_IPNLEN>	Specifies the network address and mask.

Command mode

BGP configuration mode

no-med-path-is-worst enable

Use this command to enable BGP to treat an update without a multi-exit discriminator (MED) attribute as the worst path. The default value is disable.

Syntax

no-med-path-is-worst enable

Command mode

BGP configuration mode

default no-med-path-is-worst enable

Use this command to disable BGP from treating an update without a multi-exit discriminator (MED) attribute as the worst path.

Syntax

default no-med-path-is-worst enable

Command mode

BGP configuration mode

no no-med-path-is-worst enable

Use this command to disable BGP from treating an update without a multi-exit discriminator (MED) attribute as the worst path.

Syntax

no no-med-path-is-worst enable

Command mode

BGP configuration mode

quick-start enable

Use this command to enable the quick-start flag for exponential backoff.

Syntax

quick-start enable

Command mode

BGP configuration mode

default quick-start enable

Use this command to configure the quick-start flag for exponential backoff to default.

Syntax

default quick-start enable

Command mode

BGP configuration mode

no quick-start enable

Use this command to disable the quick-start flag for exponential backoff.

Syntax

no quick-start enable

Command mode

BGP configuration mode

redistribute

Use this command to announce routes of a certain source protocol type into the BGP domain.

Syntax

redistribute <direct|ospf|rip|static>

Variable definitions

Use the following table to help you use the **redistribute <direct|ospf|rip|static>** command.

Variable	Value
enable	Enables the BGP route redistribution instance.
route-map <WORD 0-64>	Configures the route policy to apply to redistributed routes. <WORD 0-64> is an alphanumeric character string that identifies a route policy name. The character string ranges from 0 to 64 characters.

Command mode

BGP configuration mode

default redistribute

Use this command to configure BGP redistribution defaults.

Syntax

`default redistribute <direct|ospf|rip|static>`

Variable definitions

Use the following table to help you use the **`default redistribute <direct|ospf|rip|static>`** command.

Variable	Value
enable	Enables the BGP route redistribution instance.
route-map	Configures the default route policy to apply to redistributed routes.

Command mode

BGP configuration mode

no redistribute

Use this command to configure BGP redistribution defaults.

Syntax

`no redistribute <direct|ospf|rip|static>`

Variable definitions

Use the following table to help you use the **no redistribute <direct|ospf|rip|static>** command.

Variable	Value
enable	Disables the BGP route redistribution instance.
[vrf-src <WORD 0-16>]	Specifies the source VRF instance by name for route redistribution. <WORD 0-16> is an alphanumeric character string that identifies a VRF name. The character string ranges from 0 to 16 characters.

Command mode

BGP configuration mode

route-reflector enable

Use this command to enable the reflection of routes from IBGP neighbors. The default value is enable.

Syntax

route-reflector enable

Command mode

BGP configuration mode

default route-reflector enable

Use this command to enable the reflection of routes from IBGP neighbors.

Syntax

default route-reflector enable

Command mode

BGP configuration mode

no route-reflector enable

Use this command to disable the reflection of routes from IBGP neighbors.

Syntax

no route-reflector enable

Command mode

BGP configuration mode

route-refresh

Use this command to enable route refresh.

Syntax

route-refresh

Command mode

BGP configuration mode

default route-refresh

Use this command to configure route refresh to default.

Syntax

default route-refresh

Command mode

BGP configuration mode

no route-refresh

Use this command to disable route refresh.

Syntax

no route-refresh

Comments? infodev@avaya.com

Command mode

BGP configuration mode

router-id

Use this command to specify the BGP router ID in IP address format.

Syntax

router-id <A.B.C.D>

Command mode

BGP configuration mode

no router-id

Use this command to disable specifing the BGP router ID in IP address format.

Syntax

no router-id

Command mode

BGP configuration mode

synchronization

Use this command to enable the router to accept routes from BGP peers without waiting for an update from the IGP. The default value is enable..

Syntax

synchronization

Command mode

BGP configuration mode

default synchronization

Use this command to enable the router to accept routes from BGP peers without waiting for an update from the IGP. The default value is enable..

Syntax

`default synchronization`

Command mode

BGP configuration mode

no synchronization

Use this command to disable the router from accepting routes from BGP peers without waiting for an update from the IGP.

Syntax

`no synchronization`

Command mode

BGP configuration mode

traps enable

Use this command to enable BGP traps.

Syntax

`traps enable`

Command mode

BGP configuration mode

default traps enable

Use this command to configure BGP traps to default.

Syntax

`default traps enable`

Command mode

BGP configuration mode

no traps enable

Use this command to disable BGP traps.

Syntax

`no traps enable`

Command mode

BGP configuration mode

router bgp

Use this command to log in to the router BGP configuration command mode.

Syntax

`router bgp`

Command mode

Global configuration mode

no router bgp enable

Use this command to disable BGP globally.

Syntax

`no router bgp enable`

Command mode

Global configuration mode

neighbor

Use this command to configure BGP peers or peer groups.

Syntax

`neighbor <PT_IPORPEERGROUP>`

<PT_IPORPEERGROUP> specifies the peer IP address or the peer group name.

Variable definitions

Use the following table to help you use the **`neighbor <PT_IPORPEERGROUP>`** command.

Variable	Value
default-originate	Enables the switch to send a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. The default value is disable. Do not use this command if `default-information originate` is globally enabled.
enable	Enables the BGP neighbor.
in-route-map <WORD 0-256>	Applies a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates. *<WORD 0-256>* name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.
max-prefix <0-2147483647>	Sets a limit on the number of routes that can be accepted from a neighbor. The default value is 12000 routes. A value of 0 (zero) indicates that there is no limit to the number of routes that can be accepted.
MD5-authentication enable	Enables TCP MD5 authentication between two peers. The default value is disable.
neighbor-debug mask <WORD 1-100>	Displays specified debug information for a BGP peer. The default value is none. *<WORD 1-100>* is a list of mask choices separated by commas with no space

Variable	Value
	between choices. For example: *{<mask>,<mask>,<mask>...}*. Mask choices are: *none* disables all debug messages. *all* enables all debug messages. *error* enables display of debug error messages. *packet* enables display of debug packet messages. *event* enables display of debug event messages. *trace* enables display of debug trace messages. *warning* enables display of debug warning messages. *state* enables display of debug state transition messages. *init* enables display of debug initialization messages. *filter* enables display of debug messages related to filtering. *update* enables display of debug messages related to sending and receiving updates.
next-hop-self	When enabled, specifies that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. The default value is disable. The next-hop parameter can only be configured when the neighbor is disabled.
out-route-map <WORD 0-256>	Applies a route policy rule to all outgoing routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates. <*WORD 0-256*> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.
peer-group <WORD 0-1536>	Adds a BGP peer to the specified subscriber group. You must create the specified subscriber group before you issue this command.
remote-as <0-65535>	Configures the remote AS number of a BGP peer or a peer-group. You cannot configure this option when the admin-state is enable.

Variable	Value
retry-interval <1-65535>	Sets the time interval (in seconds) for the ConnectRetry Timer. The default value is 120 seconds.
route-reflector-client	Configures the specified neighbor or group of neighbors as its route reflector client. The default value is disable. All neighbors that are configured become members of the client group and the remaining IBGP peers become members of the nonclient group for the local route reflector.
route-refresh	Enables route refresh for the BGP peer. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.
send-community	Enables the switch to send the update message community attribute to the specified peer. The default value is disable.
soft-reconfiguration-in enable	When enabled, the router relearns routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable.
timers <0-21845>	Configures timers (in seconds) for the BGP speaker for this peer. *<0-21845>* is the keep alive time.
update-source <A.B.C.D>	Specifies the source IP address when BGP packets are sent to this peer or peer group. You cannot configure this parameter when the admin-state is enable. *<A.B.C.D>* is the specified source IP address.
weight <0-65535	Specifies the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer. The default value is 0. If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor.

Command mode

BGP Router Configuration mode

Comments? infodev@avaya.com

no neighbor

Use this command to disable BGP neighbor peer groups.

Syntax

no neighbor <PT_IPORPEERGROUP>

<PT_IPORPEERGROUP> specifies the peer IP address or the peer group name.

Variable definitions

Use the following table to help you use the **no neighbor <PT_IPORPEERGROUP>** command.

Variable	Value
default-originate	Prevents the switch from sending a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. The default value is disable.
enable	Disables the BGP neighbor.
in-route-map	Discontinues the application of a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates.
MD5-authentication enable	Disables TCP MD5 authentication between two peers. The default value is disable.
neighbor-debug-mask <WORD 1-100>	Discontinues displaying specified debug information for a BGP peer. <*WORD 1-100*> is a list of mask choices separated by commas with no space between choices. For example: *{<mask>,<mask>,<mask>...}*. Mask choices are: *none* disables all debug messages. *all* enables all debug messages. *error* enables display of debug error messages. *packet* enables display of debug packet messages. *event* enables display of debug event messages.

Variable	Value
	trace enables display of debug trace messages. *warning* enables display of debug warning messages. *state* enables display of debug state transition messages. *init* enables display of debug initialization messages. *filter* enables display of debug messages related to filtering. *update* enables display of debug messages related to sending and receiving updates.
next-hop-self	Discontinues specifying that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. The default value is disable. The next-hop parameter can only be configured when the neighbor is disabled.
out-route-map	Discontinues applying a route policy rule to all outgoing routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates.
peer-group	Deletes a BGP neighbor peer group.
remote-as	Deletes the BGP peer or a peer-group remote AS.
route-reflector-client	Disables the specified neighbor or neighbors route reflector clients. The default value is disable.
route-refresh	Disables route refresh for the BGP peer.
send-community	Disables the switch from sending the update message community attribute to the specified peer. The default value is disable.
soft-reconfiguration-in enable	When disabled, the router does not relearn routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable.
update-source	Disables specifying the source IP address when BGP packets are sent to this peer or

Variable	Value
	peer group. You cannot configure this parameter when the admin-state is enable.
weight	Disables specifying the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer.

Command mode

BGP Router Configuration configuration mode

default neighbor

Use this command to configure BGP peers or peer groups defaults.

Syntax

`default neighbor <PT_IPORPEERGROUP>`

<PT_IPORPEERGROUP> specifies the peer IP address or the peer group name.

Variable definitions

Use the following table to help you use the **`default neighbor <PT_IPORPEERGROUP>`** command.

Variable	Value
default-originate	Configures the BGP neighbor default-originate parameter to the default value, disable.
enable	Configures the BGP neighbor enable parameter to default.
in-route-map	Configures the BGP neighbor in-route policy to default.
max-prefix	Configures the BGP neighbor maximum prefix to the default value, 12000 routes.
MD5-authentication enable	Configures the BGP neighbor TCP MD5 authentication to the default value, disable.
neighbor-debug-mask	Configures the BGP neighbor debug information for a BGP peer to the default value, none.
next-hop-self	Configures the BGP neighbor next-hop attribute to the default value, disable.

Variable	Value
	The next-hop parameter can only be configured when the neighbor is disabled.
out-route-map	Configures the BGP neighbor outgoing route policy to the default value.
remote-as	Configures the BGP neighbor remote AS number of a BGP peer or a peer-group to the default value. You cannot configure this option when the admin-state is enable.
retry-interval	Configures the BGP neighbor time interval (in seconds) for the ConnectRetry Timer to the default value, 120 seconds.
route-refresh	Configures the BGP neighbor route refresh for the BGP peer to the default value.
send-community	Configures the switch to send the default update message community attribute to the specified peer. The default value is disable.
soft-reconfiguration-in enable	Configures the switch default for relearning routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable.
timers	Configures the BGP neighbor keep alive and hold timers (in seconds) for the BGP speaker for this peer to the default value.
update-source	Configures the source IP address when BGP packets are sent to this peer or peer group to the default value. You cannot configure this parameter when the admin-state is enable.
weight	Configures the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer to the default value, 0.

Command mode

BGP Router Configuration mode

neighbor password

Use this command to assign a BGP peer or peer group password.

Comments? infodev@avaya.com

Syntax

neighbor password <PT_IPORPEERGROUP> <WORD 0-80>

<*PT_IPORPEERGROUP*> specifies the peer IP address or the peer group name.

Variable definitions

Use the following table to help you use the **neighbor password <PT_IPORPEERGROUP> <WORD 0-80>** command.

Variable	Value
<*WORD 0-80*>	Specifies an alphanumeric string length from 0 to 80 characters.

Command mode

BGP Router Configuration mode

no neighbor password

Use this command to delete a BGP peer or peer group password.

Syntax

no neighbor password <PT_IPORPEERGROUP> <WORD 0-1536>

<*PT_IPORPEERGROUP*> specifies the peer IP address or the peer group name.

Variable definitions

Use the following table to help you use the **no neighbor password <PT_IPORPEERGROUP> <WORD 0-1536>** command.

Variable	Value
<*WORD 0-80*>	Specifies an alphanumeric string length from 0 to 80 characters.

Command mode

BGP Router Configuration mode

default neighbor password

Use this command to delete a BGP peer or peer group password.

Syntax

`default neighbor password <PT_IPORPEERGROUP> <WORD 0-1536>`

<PT_IPORPEERGROUP> specifies the peer IP address or the peer group name.

Variable definitions

Use the following table to help you use the **`no neighbor password <PT_IPORPEERGROUP> <WORD 0-1536>`** command.

Variable	Value
<WORD 0-80>	Specifies an alphanumeric string length from 0 to 80 characters.

Command mode

BGP Router Configuration mode

redistribute

Use this command to configure a redistribute entry.

Syntax

`redistribute <direct|ospf|rip|static>`

Variable definitions

The following table defines optional parameters that you enter after the **`redistribute <direct|ospf|rip|static>`** command.

Variable	Value
<cr>	Creates a redistribution instance.
enable	Enables the BGP route redistribution instance.
route-map <WORD 0-64>	Configures the route policy to apply to redistributed routes. *<WORD 0-64>* specifies an alphanumeric string length from 0 to 64 characters.

Command mode

BGP Router Configuration mode

Comments? infodev@avaya.com

default redistribute

Use this command to configure BGP redistribution defaults.

Syntax

`default redistribute <direct|ospf|rip|static>`

Variable definitions

The following table defines optional parameters that you enter after the **`default redistribute <direct|ospf|rip|static>`** command.

Variable	Value
enable	Enables the default BGP route redistribution instance.
route-map	Configures the default route policy to apply to redistributed routes.

Command mode

BGP Router Configuration mode

ip bgp apply redistribute

Use this command to apply a redistribution instance.

Syntax

`ip bgp apply redistribute <direct|ospf|rip|static>`

Command mode

Privileged EXEC mode

no redistribute

Use this command to disable a redistribute entry.

Syntax

`no redistribute <direct|ospf|rip|static> <enable>`

Variable definitions

Use the following table to help you use the **no redistribute <direct|ospf|rip|static> <enable>** command.

Variable	Value
[vrf-src <WORD 0-16>]	Specifies the source VRF instance by name for route redistribution.

Command mode

BGP Router Configuration mode

ip as-list

Use this command to configure an AS path list.

Syntax

ip as-list <1-1024> memberId <0-65535> <permit|deny> as-path <WORD 0-1536>

Variable definitions

The following table defines parameters that you enter with the **ip as-list <1-1024> memberId <0-65535> <permit|deny> as-path <WORD 0-1536>** command.

Variable	Value
<1-1024>	Specifies the AS path list ID. Values are numbers ranging from 1 to 1024.
memberId <0-65535> <permit|deny> as-path <WORD 0-1536>	Adds a regular expression entry to the specified AS path list. • memberId <0-65535> specifies an numerical identifier for the regular expression entry in the AS path list. Values range from 0 to 65535. • <permit|deny> permits or denies access for matching conditions. • as-path <WORD 0-1536> specifies a numerical identifier for the AS path. Type a single or multiple value between quotation marks (" "), for example "11" or "11 12 13". Values range from 0 to 1536.

Command mode

Global Configuration mode

no ip as-list

Use this command to delete an AS path list.

Syntax

no ip as-list <1-1024> memberId <0-65535> as-path <WORD 0-1536>

Variable definitions

The following table defines parameters that you enter with the **no ip as-list <1-1024> memberId <0-65535> as-path <WORD 0-1536>** command.

Variable	Value
<1-1024>	Specifies the AS path list ID. Values are numbers ranging from 1 to 1024.
memberId <0-65535> <permit|deny> as-path <WORD 0-1536>	Adds a regular expression entry to the specified AS path list. • memberId <0-65535> specifies an numerical identifier for the regular expression entry in the AS path list. Values range from 0 to 65535. • as-path <WORD 0-1536> specifies a numerical identifier for the AS path. Type a single or multiple value between quotation marks (" "), for example "11" or "11 12 13". Values range from 0 to 1536.

Command mode

Global Configuration mode

ip community-list

Use this command to configure a community list.

Syntax

ip community-list <1-1024> memberId <0-65535> <permit|deny> community-string <WORD 0-256>

Variable definitions

The following table defines parameters that you enter with the**ip community-list <1-1024> memberId <0-65535> <permit|deny> community-string <WORD 0-256>** command.

Variable	Value
community-list <1-1024>	Identifies the community list. Values are numbers ranging from 1 to 1024.
memberId <0-65535>	Identifies the member ID in the community list. Values are numbers ranging from 0 to 65535.
<permit|deny>	Configures the access mode to permit or deny access for matching conditions.
community-string <WORD 0-256>	An alphanumeric string of from 0 to 1536 characters in length that identifies the BGP community. You can use a numerical value or a well known community list string. Well known community strings include internet, no-export, no-advertise, and local-as.

Command mode

Global Configuration mode

no ip community-list

Use this command to delete a community list.

Syntax

no ip community-list <1-1024> memberId <0-65535> <permit|deny> community-string <WORD 0-256>

Variable definitions

The following table defines parameters that you enter with the**no ip community-list <1-1024> memberId <0-65535> <permit|deny> community-string <WORD 0-256>** command.

Variable	Value
community-list <1-1024>	Identifies the community list. Values are numbers ranging from 1 to 1024.
memberId <0-65535>	Identifies the member ID in the community list. Values are numbers ranging from 0 to 65535.

Comments? infodev@avaya.com

Variable	Value
community-string <WORD 0-256>	An alphanumeric string of from 0 to 1536 characters in length that identifies the BGP community. You can use a numerical value or a well known community list string. Well known community strings include internet, no-export, no-advertise, and local-as.

Command mode

Global Configuration mode

ip bgp restart-bgp

Use this command to restart BGP.

Syntax

`ip bgp restart-bgp`

Variable definitions

The following table defines optional parameters that you enter after the **`ip bgp restart-bgp`** command.

Variable	Value
neighbor <PT_IPORPEERGROUP>	Restarts BGP for a specific BGP peer or peer group.
vrf [WORD <0-16>]	Specifies a VRF instance by name. Value is a character string with a maximum of 16 characters.

Command mode

Privileged EXEC mode

ip bgp stats-clear-counters

Use this command to clear BGP stastical counters.

Syntax

`ip bgp stats-clear-counters`

Command mode

Global Configuration mode

ip bgp stats-clear-counters neighbor

Use this command to clear BGP neighbor stastical counters.

Syntax

ip bgp stats-clear-counters neighbor <PT_IPORPEERGROUP>

Variable definitions

The following table defines parameters that you enter with the **ip bgp stats-clear-counters neighbor <PT_IPORPEERGROUP>** command.

Variable	Value
neighbor <PT_IPORPEERGROUP>	Restarts BGP for a specific BGP peer or peer group.

Command mode

Global Configuration mode

show ip bgp aggregates

Use this command to display information about current aggregate addresses.

Syntax

show ip bgp aggregates [<PT_IPNLEN>]

[<PT_IPNLEN>] specifies the IP address and the mask length. Values for mask length range from 0 to 32.

Command mode

Privileged EXEC mode

show ip bgp cidr-only

Use this command to display information about classless interdomain routing (CIDR) routes.

Syntax

show ip bgp cidr-only [<PT_IPNLEN>]

[<PT_IPNLEN>] specifies the IP address and the mask length. Values for mask length range from 0 to 32.

Command mode

Privileged EXEC mode

show ip bgp conf

Use this command to view the global BGP configuration.

Syntax

show ip bgp conf

Command mode

Privileged EXEC mode

show ip bgp neighbors

Use this command to display information about BGP peers.

Syntax

show ip bgp neighbors

OR

show ip bgp neighbors <A.B.C.D>

Variable definitions

The following table defines parameters that you enter after the**show ip bgp neighbors <A.B.C.D>** command.

Variable	Value
<*A.B.C.D*>	Identifies a specific BGP neighbor IP address.
advertised-routes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).

Variable	Value
routes	Shows paths with this prefix for nonIP VPN routes. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
stats	Displays BGP neighbor statistical information.
vrf	Specifies a VRF instance by name. Value is a character string with a maximum of 16 characters.
vrfids	Specifies a VRF ID number. Values are alphanumeric characters ranging from 0 to 255.

Command mode

Privileged EXEC mode

show ip bgp networks

Use this command to view BGP network configurations.

Syntax

show ip bgp networks [<PT_IPNLEN>]

[<PT_IPNLEN>] specifies the IP address and the mask length. Values for mask length range from 0 to 32.

Command mode

Privileged EXEC mode

show ip bgp peer-group

Use this command to display information about BGP peer groups.

Syntax

show ip bgp peer-group [<WORD 1-1536>]

[<WORD 1-1536>] specifies the peer group name. Values are alphanumeric characters ranging from 1 to 1536 characters.

Command mode

Privileged EXEC mode

show ip bgp route

Use this command to view BGP route information.

Syntax

`show ip bgp route <PT_IPNLEN>`

<*PT_IPNLEN*> specifies the IP address and the mask length. Values for mask length range from 0 to 32.

Variable definitions

The following table defines optional parameters that you enter after the **`show ip bgp route <PT_IPNLEN>`** command.

Variable	Value
[community <enable|disable>]	Enables or disables the display of community attributes.
[ip <A.B.C.D>]	Specifies an IP address.
[longer-prefixes]	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).

Command mode

Privileged EXEC mode

show ip bgp redistributed-routes

Use this command to display information about BGP routes.

Syntax

`show ip bgp redistributed-routes`

Variable definitions

The following table defines optional parameters that you enter after the **`show ip bgp redistributed-routes`** command.

Variable	Value
<PT_IPNLEN>	Specifies the IP address and the mask length. Values for mask length range from 0 to 32.

Command mode

Privileged EXEC mode

show ip bgp summary

Use this command to display summarized information about BGP.

Syntax

show ip bgp summary

Command mode

Privileged EXEC mode

show ip bgp stats

Use this command to display bgp statistical information.

Syntax

show ip bgp stats

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

Chapter 19: Show commands

This chapter describes ACLI show commands and their parameters.

Navigation

- show vct on page 487
- show poe main-status|port-stats|port-status|power-measurement|sys-status on page 488
- show web-server on page 488
- show qos egress-counter-set|egress-stats|mac-qos-level-override|map|policy|policy-remark-dp|policy-stats on page 489
- show ip pim active-rp|bsr|interface|mode|mroute|neighbor|rp-candidate|rp-hash|static-rp|virtual-neighbor on page 490
- show debug ip pim on page 491
- show interfaces vlan ip on page 491
- show ip igmp on page 492
- show ip igmp interface vlan on page 494
- show ip igmp multicast-vlan-registration group on page 494
- show ip igmp multicast-vlan-registration vlan on page 495
- show ip dhcp-relay fwd-path on page 495
- show ip dhcp-relay interface on page 496
- show ip dhcp-relay counters on page 496
- show ip mroute interface|next-hop|route|static-source-group on page 498
- show interface FastEthernet|GigabitEthernet|Loopback|vlan on page 500
- show rmon on page 502
- show spanning-tree config|port|status on page 502
- show test on page 503
- show sys-info on page 503
- show trace file on page 504

- show trace level on page 504
- monitor mlt error collision on page 505
- monitor mlt error main on page 505
- monitor mlt stats interface main on page 505
- monitor mlt stats interface utilization on page 506
- monitor ports error collision on page 506
- monitor ports error extended on page 506
- monitor ports error main on page 507
- monitor ports statistics interface extended on page 507
- monitor ports statistics interface main on page 508
- monitor ports statistics interface utilization on page 509
- monitor ports statistics rmon on page 509
- monitor ports statistics stp on page 510
- show filter acg on page 510
- show filter acl action on page 511
- show filter acl ethernet on page 511
- show filter acl ip on page 511
- show filter acl protocol on page 512
- show filter acl statistics on page 512
- show filter act ethernet on page 512
- show filter act ip on page 513
- show mlt on page 513
- show mlt error on page 513
- show mlt error collision on page 514
- show smlt on page 514
- show ip rsmlt on page 514
- show ist on page 515
- show ist stat on page 515
- show mlt stats on page 515
- show interface vlan on page 516
- show vlan advance on page 516
- show ip arp interface on page 516

- show vlan autolearn-mac on page 517
- show vlan vid basic on page 517
- show vlan vid fdb-entry on page 517
- show vlan vid fdb-filter on page 518
- show vlan vid fdb-static on page 518
- show interfaces vlan ip on page 518
- show vlan manual-edit-mac on page 519
- show vlan members on page 519
- show vlan static-mcastmac on page 519
- show interface loopback on page 520
- show ip arp on page 520
- show ip forward-protocol udp on page 520
- show ip global on page 521
- show ip interface on page 521
- show ip irdp on page 522
- show ip ospf on page 522
- show ip ospf accept on page 523
- show ip ospf area on page 523
- show ip ospf ase on page 524
- show ip ospf authentication interface on page 524
- show ip ospf default-cost on page 525
- show ip ospf host-route on page 525
- show ip ospf ifstats on page 525
- show ip ospf int-auth on page 526
- show ip ospf int-timers on page 526
- show ip ospf interface on page 526
- show ip ospf lsdb on page 527
- show ip ospf neighbours interface on page 528
- show ip ospf redistribute on page 528
- show ip ospf stats on page 528
- show ip ospf timer interface on page 529
- show ipv6 global on page 529

- show ipv6 address ip on page 530
- show ipv6 route on page 530
- show ipv6 neighbor on page 531
- show ipv6 interface on page 531
- show ipv6 nd-prefix [detail] on page 532
- show ip prefix-list on page 532
- show ip rip on page 532
- show ip rip interface on page 533
- show ip routing on page 533
- show route-map on page 533
- show ip route on page 534
- show ip tcp on page 535
- show lldp on page 535
- show slpp on page 537
- show ports stats dhcp-relay on page 537
- show vlan nlb-mode on page 537
- show snmp-server on page 538
- show eapol on page 538
- show access-policy on page 539
- show nsna on page 539
- show nsna client on page 539
- show nsna nsnas on page 540
- show nsna interface on page 540
- show nsna phone-signature on page 541
- show nsna vlan on page 541
- show radius on page 541
- show radius-server on page 542
- show sys log host on page 542
- show boot config on page 543
- show boot config choice on page 544
- show boot config cli on page 544
- show boot config config on page 544

- show boot config flags on page 544
- show boot config host on page 545
- show boot config info on page 545
- show boot config master on page 545
- show boot config net on page 546
- show boot config sio on page 546
- show boot config tz on page 546
- show autotopology on page 546
- show basic config on page 547
- show interfaces GigabitEthernet interface on page 547
- show link-flap-detect on page 547
- show logging config on page 548
- show logging file on page 548
- show log filter on page 549
- show running-config on page 549
- show slot on page 549
- show sys hash-calc mltindex ip dest-mac dest-ip src-mac src-ip src-port mlt on page 550
- show sys hash-calc mltindex non-ip dest-mac src-mac src-port mlt on page 551
- show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt on page 551
- show sys hash-calc mltindex non-ip-mcast dest-mac vlan-id src-port mlt on page 552
- show sys-info on page 553
- show sys perf on page 553
- show sys sw on page 554
- show ip vrf on page 554

show vct

This command displays a virtual cable test or displays Virtual Cable Tester (VCT) information for a range of ports.

Syntax

show vct *<portlist>*

Variable definitions

Use the following table to help you use the **show vct** command.

Variable	Value
<portlist>	Displays a virtual cable test on the specified ports. *portlist* specify the ports in the portlist form *{ slot/port [- slot/port][, ...]}*.

Command mode

Privileged EXEC mode

show poe main-status|port-stats|port-status|power-measurement|sys-status

Use this command to show the poe status by slot.

Syntax

show poe <main-status|port-stats|port-status|power-measurement|sys-status> [slot *<slot id>* **]**

Variable definitions

Use the following table to help you use the **show poe** command.

Variable	Value
main-status	Shows the card power information.
port-stats	Shows the port power statistics.
port-status	Shows the port power information.
power-measurement	Shows the port power measurement.
sys-status	Shows the system power information.

Command mode

Privileged Exec mode

show web-server

Use this command to display whether the Web access is enabled, and to display the password and access information.

Syntax

show web-server

Command mode

Privileged EXEC mode

---

show qos egress-counter-set|egress-stats|mac-qos-level-override|map|policy|policy-remark-dp|policy-stats

Use this command to display information about the QoS (Quality of Service).

Syntax

show qos <egress-counter-set|egress-stats|mac-qos-level-override|map|policy|policy-remark-dp|policy-stats> *[<1-40>* **]**

Variable definitions

The following table describes the variable that you use with the **show qos** command.

Variable	Value
egress-counter-set	Displays the qos tx queue counter set configuration.
egress-stats	Displays the qos tx queue counters.
mac-qos-level-override	Displays mac-qos-level-override.
map	Displays the QoS mapping tables.
policy	Displays the information about QoS policies.
policy-remark-dp	Displays the status of the policy remark dp configuration.
policy-stats	Displays the information about QoS policy statistics.

Variable definitions

The following table describes the optional parameters that you use with the **show qos** command.

Variable	Value
8021p-to-class-map	Displays 802.1p value to traffic class.
8021p-to-drop-precedence-map	Displays 802.1p value to drop precedence.
8021p-to-dscp-map	Displays 802.1p to dscp map.

Variable	Value
class-to-8021p-map	Displays traffic class to 802.1p value..
class-to-8021p-policied-map	Displays traffic class to 8021p based on conformance level.
class-to-dscp-policied-map	Displays traffic class to 8021p based on conformance level.
dscp-to-cos-policied-map	Displays dscp to cos parameters based on conformance level.
<0-128>	Indicates the QoS policy id which is in the range of 0 to 128.
<1-40>	This the QoS counter id in the range of 1 to 40.

Command mode

Privileged EXEC mode

show ip pim active-rp|bsr|interface|mode|mroute|neighbor|rp-candidate|rp-hash|static-rp|virtual-neighbor

Use this command to display information about the active rendezvous point (RP) for a specific group.

Syntax

`show ip pim [<active-rp|bsr|interface|mode|mroute|neighbor|rp-candidate|rp-hash|static-rp|virtual-neighbor><A.B.C.D>]`

Variable definitions

Use the following table to help you use the **`show ip pim`** command.

Variable	Value
active-rp	Displays configuration settings for active-rp.
bsr	Displays configuration information for a bootstrap router.
interface	Displays configuration information about a particular PIM-SM interface.
mode	Displays configuration information setting for a particular mode.
mroute	Displays configuration settings for a particular route.

Variable	Value
neighbor	Displays configuration settings for a PIM-SM neighbor.
rp-candidate	Displays candidates RP information.
rp-hash	Displays configuration settings for RP candidate.
static-rp	Displays configuration settings for static-rp.
virtual-neighbor	Displays information about the neighboring routers configured with PIM-SM.
{A.B.C.D}	IP address of a multicast group.

Command mode

Privileged EXEC mode

show debug ip pim

Use this command to display the current PIM-SM debug trace flag settings on the switch.

Syntax

`show debug ip pim`

Command mode

Privileged EXEC mode

show interfaces vlan ip

This command allows you to view the IP VLAN interfaces.

Syntax

`show interfaces vlan ip [<1-4000>]`

Variable definitions

Use the following table to help you use the **`show interfaces vlan ip`** command.

Variable	Value
<1-4000>	This is the vlan id in the range of 1 to 4000. Any value between 1 and 2000 will be a default value.

Command mode

Privileged EXEC mode

show ip igmp

Use this command to display information about IGMP.

Syntax

`show ip igmp`

Variable definitions

Use the following table to help you use the **`show ip igmp`** command.

Variable	Value
access	Displays information about IGMP multicast access filters.
cache	Displays information about IGMP cached groups.
[<count>]group [<count>]	Displays information about IGMP groups per port.
interface	Displays information about the IGMP interface (i.e., the IGMP querier).
mrdisc	Displays information about the multicast router discovery.
router-alert	Displays the IGMP router alert check status.
[]sender [<count>]	Displays information about the IGMP sender list.
snoop	Displays the status of IGMP snoop and proxy-snoop.
static	Displays information about the static and blocked ports for the IGMP-enabled interfaces.
stream-limit	Displays multicast stream limitation members on an interface.
sys	Displays the IGMP system parameters.

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

show ip igmp ssm

Use this command to display the SSM global configuration.

Syntax

show ip igmp ssm

Command mode

Privileged EXEC Configuration mode

show ip igmp ssm-map

Use this command to display the SSM channel table.

Syntax

show ip igmp ssm-map

Command mode

Privileged EXEC Configuration mode

show ip arp-inspection vlan

Use this command to view dynamic ARP inspection configuration.

Syntax

show ip arp-inspection vlan

Command mode

User EXEC mode

show ip arp-inspection interface

Use this command to view port dynamic ARP inspection status.

Syntax

show ip arp-inspection interface

Variable definitions

The following table defines parameters that you enter with the **show ip arp-inspection interface** command.

Variable	Value
<cr>	Displays port dynamic ARP inspection status for all interface ports on the switch
<interface type>	Identifies a specific type of interface for which to display port ARP inspection status. Values are FastEthernet and GigabitEthernet.
<port>	Specifies the port number for a single port or range of ports, entered as {slot/port[-slot/port][,...]}.

Command mode

User EXEC mode

show ip igmp interface vlan

Use this command to display information about the Internet Group Management Protocol (IGMP) operation for a Virtual LAN (VLAN) on the switch.

Syntax

show ip igmp interface vlan <*vid*>

Command mode

Privileged EXEC mode

For more information about VLAN operations, see *Avaya Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the ACLI, NN46200-504*.

show ip igmp multicast-vlan-registration group

Use this command to view MVR group information to verify the configuration and troubleshoot.

syntax

show ip igmp multicast-vlan-registration group [vlan<1-4000>] [address<A.B.C.D>]

Comments? infodev@avaya.com

Variable definitions

Use the data in the following table to help you use **show ip igmp multicast-vlan-registration group** command.

Variable	Value
<cr>	Shows all groups.
vlan <1-4000>	Specifies the VLAN to which the group belongs. Vvalue is the VLAN ID in the range of 1–4000.
address <A.B.C.D>	Specifies the IP address of a specific group. Value is the IP address in the format of A.B.C.D.

Command mode

Privileged EXEC mode

show ip igmp multicast-vlan-registration vlan

Use this command to view multicast VLAN information to see the VLANS that are bound to the MVR VLAN.

syntax

show ip igmp multicast-vlan-registration vlan

Command mode

Privileged EXEC mode

show ip dhcp-relay fwd-path

Use this command to display information about DHCP relay forward path.

syntax

show ip dhcp-relay fwd-path [vrf<WORD 0-32>][vrfids<WORD 0-127>]

Variable definitions

Use the data in the following table to help you use **show ip dhcp-relay fwd-path** command.

Variable	Value
[vrf <WORD/0-32>	Specifies the name of the VRF.

Variable	Value
[vrfids <WORD/0-127>	Specifies the ID of the VRF and is an integer in the range of 0–127.

Command mode

Privileged EXEC mode

show ip dhcp-relay counters

Use this command to display information about DHCP relay counters.

syntax

show ip dhcp-relay counters [vrf<WORD 0-32>][vrfids<WORD 0-127>]

Variable definitions

Use the data in the following table to help you use **show ip dhcp-relay counters** command.

Variable	Value
[vrf <WORD/0-32>	Specifies the name of the VRF.
[vrfids <WORD/0-127>	Specifies the ID of the VRF and is an integer in the range of 0–127.

Command mode

Privileged EXEC mode

show ip dhcp-relay interface

Viewing DHCP relay information for a port or a VLAN to verify the configuration and to troubleshoot.

syntax

show ip dhcp-relay interface [Vlan<1-4000>] [vrf <WORD 0-32>] [vrfids <WORD 0-127>]

Variable definitions

Use the data in the following table to help you use **show ip dhcp-relay interface** command.

Variable	Value
Vlan<1-4000>	Specifies the ID of the VLAN in the range of 1–4000.
vrf <WORD 0-32>	Specifies the name of the VRF.
vrfids <WORD 0-127>	Specifies the ID of the VRF and is an integer in the range of 0–255.

Command mode

Privileged EXEC mode or VRF Router mode

show ip dhcp-snooping

Use this command to view the global DHCP snooping status.

Syntax

show ip dhcp-snooping

Command mode

User EXEC mode

show ip dhcp-snooping vlan

Use this command to view VLAN-based DHCP snooping status.

Syntax

show ip dhcp-snooping vlan

Command mode

User EXEC mode

show ip dhcp-snooping binding

Use this command to view DHCP snooping binding information.

Syntax

show ip dhcp-snooping binding

Command mode

User EXEC mode

show ip ipfix

Use this command to .

Syntax

show ip ipfix

Variable definitions

The following table describes optional parameters that you enter after the **show ip ipfix** command.

Variable	Value
<cr>	Displays global IPFIX configuration information.
collector <ipaddr>	Displays the IPFIX collector information for the switch or a specific collector IP address.
export	Displays IPFIX exporter statistics information.
exporter	Displays IPFIX exporter configuration information.
flows	Displays the IPFIX flow table.
interface	Displays IPFIX interface information.

Command mode

Privileged EXEC configuration mode

show ip mroute interface|next-hop|route|static-source-group

Use this command to display information about the static source-groups on the current interface.

Syntax

show ip mroute [<interface|next-hop|route|static-source-group><A.B.C.D>]

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`show ip mroute`** command.

Variable	Value
interface	Displays mroute interface information.
next-hop	Displays mroute next-hop information.
route	Displays mroute route information.
static-source-group	Displays mroute static-source-group information.

Command mode

Privileged EXEC mode

show ip verify source

Use this command to display the IP Source Guard configuration for all switch interface ports, a specific interface port, or a range of interface ports.

Syntax

`show ip verify source`

Variable definitions

The following table defines parameters that you enter with the **`show ip verify source`** command.

Variable	Value
<cr>	Displays IP Source Guard configuration information for all switch interface ports
interface <interface type>	Identifies a specific type of interface for which you want to view IP Source Guard configuration information. Values are FastEthernet and GigabitEthernet.
<portlist>	Specifies a single port or range of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Privileged Exec mode

show ip source binding

Use this command to display binding information all interface ports on the switch, a single interface port, or a range of interface ports.

Syntax

`show ip source binding`

Variable definitions

The following table defines parameters that you enter with the **`show ip source binding`** command.

Variable	Value
<A.B.C.D>	Identifies the IP address or group of addresses that IP Source Guard allowed.
interface <interface type>	Identifies a specific type of interface for which you want to view IP Source Guard binding information. Values are FastEthernet and GigabitEthernet.
<portlist>	Specifies a single port or range of ports, entered as {slot/port[-slot/ port][,...]}.

Command mode

Privileged Exec mode

show interface FastEthernet|GigabitEthernet|Loopback|vlan

Use this command to display information about the ports on the switch.

Syntax

`show interface <FastEthernet|GigabitEthernet|Loopback|vlan>`

Variable definitions

Use the following table to help you use the **`show interface`** command.

Variable	Value
config [*<ports>*]	Displays general configuration information about all ports or about specified ports.

Comments? infodev@avaya.com

Variable	Value
cp-limit	Displays the port packet cp-limit commands.
eapol [<*ports*>]	Displays Extensible Authorization Protocol (EAP) information about all ports or about specified ports. There are 5 options: • auth-diags • auth-stats • config • oper-stats • session-stats
error [<*ports*>]	Displays general error information about all ports or about specified ports.
igmp [<*ports*>]	Displays Internet Group Management Protocol (IGMP) information about all ports or about specified ports.
interface [<*ports*>]	Displays information about the physical interface for all ports or for specified ports.
name [<*ports*>]	Displays general information, including the name or names for all ports or for specified ports.
qos [<*ports/slots*>]	Displays Quality of Service (QoS) information about all ports or about specified ports.
statistics	Displays the port statistics information.
tx-queue [<*ports*>]	Displays the transmit queue for all ports or for specified ports.
unknown-mac-discard [<*ports*>]	Displays settings for the unknown MAC discard feature for all ports or for specified ports.
vlan	Displays port vlan information.
vrf	Displays loopback configuration information for a particular vrf.
vrfids	Displays loopback configuration information for vrfids.

Command mode

Privileged EXEC mode

show rmon

Use this command to display various Remote Monitoring (RMON) settings.

Syntax

show rmon

Variable definitions

Use the following table to help you use the **show rmon** command.

Variable	Value
alarm	Displays the RMON Alarm table entries.
event	Displays the RMON event table entries.
history	Displays the RMON history control table entries.
log	Displays the RMON log table entries.
stats	Displays the RMON statistics table entries.

Command mode

Privileged EXEC mode

show spanning-tree config|port|status

Use this command to display the Spanning-Tree Group (STG) status and configuration for the specified STG.

Syntax

show spanning-tree [<config|port|status|stp>]

Variable definitions

Use the following table to help you use the **show spanning-tree [<config|port|status|stp>]** command.

Variable	Value
config	Displays spanning-tree configuration and status.
port	Displays spanning-tree status of each port.
status	Displays spanning-tree status.

Variable	Value
stp	Specifies the spanning-tree id and is in the range of 1 to 64.

Command mode

Privileged EXEC mode

show test

Use this command to display test results for the switch.

Syntax

show test [loopback [*<portlist>* **]]**

Variable definitions

Use the following table to help you use the **show test [loopback]** command.

Variable	Value
loopback [*<portlist>*]	Displays the results of the latest loopback test for the switch or for the specified port or ports.

Command mode

Privileged EXEC mode

show sys-info

Use this command to display system information about status, hardware, software, and operation of the switch. The information available from the **show sys-info** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and modules), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), OSPF (area, interface, neighbors), and log and trace files.

Syntax

show sys-info [asic] [card] [mda]

Variable definitions

Use the following table to help you use the **show sys-info** command.

Variable	Value
asic	Displays detailed information about the Application Specific Integrated Circuit (ASIC) trays in the switch.
card	Displays detailed information about the cards in the switch.
mda	Displays detailed information about the Media Dependent Adapters (MDAs) in the switch.

Command mode

Privileged EXEC mode

show trace file

Use this command to display the trace message file when tracing is enabled.

Syntax

`show trace file [tail]`

[tail] is an optional parameter that displays the log file in reverse order with the most recent information first.

Command mode

Privileged EXEC mode

show trace level

Use this command to display trace information for the switch.

Syntax

`show trace level`

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

monitor mlt error collision

Use this command to monitor the number and type of Ethernet collision errors for all Multilink Trunks (MLT) or for a specified MLT. Sample interval and duration are set by the monitor command in Global configuration mode.

Syntax

monitor mlt error collision [<*mid*> **]**

<*mid*> is an optional parameter that specifies the MLT ID. Values range from 1 to 31.

Command mode

Privileged EXEC mode

monitor mlt error main

Use this command to monitor basic information about the number of different types of Ethernet errors for all Multilink Trunks (MLT) or for a specified MLT.

Syntax

monitor mlt error main [<*mid*> **]**

<*mid*> is an optional parameter that specifies the MLT ID.

Command mode

Privileged EXEC mode

monitor mlt stats interface main

Use this command to monitor interface statistics for all Multilink Trunking (MLT) or a specified MLT.

Syntax

monitor mlt stats interface main [<*mid*> **]**

<*mid*> is an optional parameter that specifies the MLT ID.

Command mode

Privileged EXEC mode

monitor mlt stats interface utilization

Use this command to monitor interface utilization statistics for all Multilink Trunking (MLT) or for a specified MLT.

Syntax

monitor mlt stats interface utilization [<*mid*> **]**

<*mid*> is an optional parameter that specifies the MLT ID.

Command mode

Privileged EXEC mode

monitor ports error collision

Use this command to monitor the number and type of Ethernet collision errors for all ports or for specified ports.

Syntax

monitor ports error collision [<*ports*> **] [from** <*value*> **]**

Variable definitions

Use the following table to help you use the **monitor ports error collision** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

monitor ports error extended

Use this command to monitor additional information about Ethernet errors for all ports or for specified ports.

Comments? infodev@avaya.com

Syntax

monitor ports error extended [<*ports*> **] [from** <*value*> **]**

Variable definitions

Use the following table to help you use the **monitor ports error extended** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

monitor ports error main

Use this command to monitor basic information about the number of different types of Ethernet errors for all ports or for specified ports.

Syntax

monitor ports error main[<*ports*> **] [from** <*value*> **]**

Variable definitions

Use the following table to help you use the **monitor ports error main** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

monitor ports statistics interface extended

Use this command to monitor extended port interface statistics for all ports or for specified ports.

Syntax

monitor ports statistics interface extended [<*ports*> **] [from** <*value*> **]**

Variable definitions

Use the following table to help you use the **monitor ports statistics interface extended** command.

Variable	value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

monitor ports statistics interface main

Use this command to monitor basic port interface statistics for all ports or for specified ports.

Syntax

monitor ports statistics interface main [<*ports*> **] [from** <*value*> **]**

Variable definitions

Use the following table to help you use the **monitor ports statistics interface main** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

monitor ports statistics interface utilization

Use this command to monitor port interface utilization statistics for all ports or for specified ports.

Syntax

monitor ports statistics interface utilization [<*ports*> **] [from** <*value*> **]**

Variable definitions

Use the following table to help you use the **monitor ports statistics interface utilization** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

monitor ports statistics rmon

Use this command to monitor Remote Network Monitoring (RMON) statistics for all ports or for specified ports.

Syntax

monitor ports statistics rmon [<*ports*> **] [from** <*value*> **]**

Important:
RMON must be enabled on the port or ports to be monitored.

Variable definitions

Use the following table to help you use the **monitor ports statistics rmon** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

monitor ports statistics stp

Use this command to monitor Spanning Tree Protocol (STP) statistics for all ports or for specified ports.

Syntax

`monitor ports statistics stp [` <*ports*> **`] [from`** <*value*> **`]`**

Variable definitions

Use the following table to help you use the **`monitor ports statistics stp`** command.

Variable	Value
[<*ports*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.
[from <*value*>]	Specifies the port(s) to be monitored in the port list form: *{slot/port [-slot/port][, ...]}*.

Command mode

Privileged EXEC mode

show filter acg

Use this command to display the list of ACGs configured on the switch.

Syntax

`show filter acg [<acg-id>]`

<*acl-id*> is a access group identifier (from 1 to 1024) for this ACG entry.

Command mode

Global configuration mode

Comments? infodev@avaya.com

show filter acl action

Use this command to display the list of ACLs and their related ACE actions.

Syntax

show filter acl action [<acl-id>]

<*acl-id*> is a access control identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter acl ethernet

Use this command to display information about the Ethernet ACEs.

Syntax

show filter acl ethernet [<acl-id>]

<*acl-id*> is a access control identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter acl ip

Use this command to display information about the IP ACEs.

Syntax

show filter acl ip [<acl-id>]

<*acl-id*> is a access control identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter acl protocol

Use this command to display information about the ACEs protocols.

Syntax

show filter acl protocol [<acl-id>]

<*acl-id*> is a unique identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter acl statistics

Use this command to display the ACE statistics.

Syntax

show filter acl statistics [<acl-id>]

<*acl-id*> is a unique identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter act ethernet

Use this command to display information about the Ethernet ACTs.

Syntax

show filter act ethernet [<acl-id>]

<*acl-id*> is a unique identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter act ip

Use this command to display information about the IP ACTs.

Syntax

show filter act ip [<acl-id>]

<*acl-id*> is a unique identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show mlt

Use this command to display information about MultiLink Trunking (MLT) operation on the switch or the status of a specified MLT.

Syntax

show mlt [<*mid*> **]**

[mid] specifies the MLT ID. Values range from 1 to 31.

Command mode

Privileged EXEC mode

show mlt error

Use this command to display information about the types of Ethernet errors sent and received by all configured MultiLink Trunks (MLTs) or for the specified MLT.

Syntax

show mlt error [<*mid*> **]**

<*mid*> specifies the MLT ID. Values range from 1 to 31.

Command mode

Privileged EXEC mode

show mlt error collision

Use this command to display the number and type of Ethernet collision errors for all configured MultiLink Trunks (MLTs) or for the specified MLT.

Syntax

show mlt error collision [<*mid*> **]**

<*mid*> specifies the MLT ID. Values range from 1 to 31.

Command mode

Privileged EXEC mode

show smlt

This command shows the SMLT and single-port SMLT configurations on the switch.

Syntax

show smlt <mlt | fastethernet>

Variable definitions

Use the following table to help you use the **show smlt <mlt|fastethernet>** command.

Parameter	Description
mlt	Displays only the MLT-based SMLTs.
fastethernet	Displays only the port-based SMLTs.

show ip rsmlt

Use this command to display RSMLT information about a interface.

syntax

show ip rsmlt [<local|peer>]

Variable definitions

Use the data in the following table to help you use **show ip rsmlt** command.

Comments? infodev@avaya.com

Variable	Value
[<local|peer>]	Indicates a configuration for a local or peer device.

Command mode

VRF Router configuration mode

show ist

This command shows the IST configuration on the switch.

Syntax

show ist

Command mode

User Exec mode

show ist stat

This command shows the IST statistics for the switch.

Syntax

show ist stat

Command mode

User Exec mode

show mlt stats

Use this command to display statistics about MultiLink Trunking (MLT) operation on the switch or statistics for a specified MLT.

Syntax

show mlt stats [<*mid*> **]**

<*mid*> specifies the MLT ID. Values range from 1 to 31.

Command mode

Privileged EXEC mode

show interface vlan

Use this command to display protocol, configuration, and parameter information for all Virtual LANs (VLANs) on the switch or for a specified or VLAN.

Syntax

show interface vlan [*<vid>* **]**

[vid <vid>] specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Privileged EXEC mode

show vlan advance

Use this command to display protocol, configuration, and parameter information all Virtual LANs (VLAN) for a specified VLAN.

Syntax

show vlan vid <vid> advance

[vid <vid>] specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Global configuration mode

show ip arp interface

Use this command to display Address Resolution Protocol (ARP) configurations for all Virtual LANs (VLANs) on the switch or for a specified VLAN.

Syntax

show ip arp interface[*<vid>* **]**

[vid <vid>] specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Privileged EXEC mode

show vlan autolearn-mac

Use this command to display the Mac addresses that were autolearned for the switch.

Syntax

`show vlan autolearn-mac`

Command mode

Global configuration mode

show vlan vid basic

Use this command to display the basic Mac addresses for the switch.

Syntax

`show vlan [vid` <*vid*> **`] basic`**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Global configuration mode

show vlan vid fdb-entry

Use this command to display forwarding database information for the specified Virtual LAN (VLAN).

Syntax

`show vlan vid` <*vid*> **`fdb-entry`**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Global configuration mode

show vlan vid fdb-filter

Use this command to display the forwarding database filters for the specified Virtual LAN (VLAN).

Syntax

show vlan vid <*vid*> **fdb-filter**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Global configuration mode

show vlan vid fdb-static

Use this command to display the forwarding database MAC addresses that have been manually (statically) configured by the user. This is used in situations where the device does not actively advertise its address. For example, a device that does not participate in ARP.

Syntax

show vlan vid <*vid*> **fdb-static**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Global configuration mode

show interfaces vlan ip

Use this command to display the Internet Protocol (IP) address configuration for all Virtual LANs (VLANs) on the switch or for a specified VLAN.

Syntax

show interfaces vlan ip [<*vid*> **]**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Privileged EXEC mode

Comments? infodev@avaya.com

show vlan manual-edit-mac

Use this command to display the manually entered Media Access Control (MAC) addresses and their associated ports.

Syntax

show vlan manual-edit-mac

Command mode

User EXEC mode

show vlan members

Use this command to display Virtual LAN (VLAN) information for a specified port or ports.

Syntax

show vlan [vid <*vid*> **] members**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Global configuration mode

show vlan static-mcastmac

Use this command to display the Layer 2 multicast Media Access Control (MAC) filters for any Virtual LANs (VLANs) on the switch or for a specified VLAN.

Syntax

show vlan [vid <*vid*> **] static-mcastmac**

[vid <vid>] specifies the VLAN ID. Values range from 1 to 4000.

Command mode

Privileged EXEC mode

show interface loopback

This command allows you to view the CLIP interfaces, enter the following command in any mode:

Syntax

show interface loopback <vrf|vrfids>

<*vrf*|*vrfids*> display loopback configurations for a particular vrf or vrfids.

Command mode

User EXEC mode

show ip arp

Use this command to display the Address Resolution Protocol (ARP) table.

Syntax

show ip arp [ip <*ipaddr*> **] [-s** <*value*> **]**

Variable definitions

Use the following table to help you use the **show ip arp** command.

Variable	Value
[<*ipaddress*>]	Specifies the selected net IP address for the table.
[-s <value>][-s<value>]	Specifies the selected subnet in the format: {a.b.c.d/x | a.b.c.d/x.x.x.x | default}

Command mode

Interface configuration mode

show ip forward-protocol udp

This command allows you to view the existing UDP forwarding protocol.

Syntax

show ip forward-protocol udp <interface|portfwd|portfwdlist|vrf|vrfids>

Comments? infodev@avaya.com

Variable definitions

Use the following table to help you use the **`show ip forward-protocol udp`** command.

Variable	Value
interface	Displays all UDP forwarding policies together with settings and general usage statistics for each forwarding policy.
portfwd	Displays port forward information.
portfwdlist	Displays a list of all udp forwardng policies.
vrf	Displays udp configuration information for a particular vrf.
vrfids	Enter vrfids.

Command mode

Privileged EXEC mode

show ip global

Use this command to display the global IP configuration settings.

Syntax

`show ip global`

Command mode

Privileged Exec mode

show ip interface

Use this command to display the IP interfaces on the switch.

Syntax

`show ip interface`

Command mode

Privileged EXEC mode

show ip irdp

Use this command to view the router discovery status.

Syntax

`show ip irdp <interface|vrf|vrfids>`

Variable definitions

The following table describes the variables that you use in the **`show ip irdp`** command.

Variable	Value
interface	Shows route discovery for each interface information.
vrf	Shows route discovery for a particular vrf.
vrfids	Shows route discovery for a particular vrf id.

Variable definitions

The following table describes the optional parametersthat you use in the **`show ip irdp`** command.

Variable	Value
fastethernet|gigabitethernet	Displays port route discovery information.
vlan <1-4000>	Displays the router discovery status on VLANs. <1-4000> is the vlan id.
WORD <0-16>	This is the vrf name
WORD <0-127>	This is the vrf id.

Command mode

Privileged EXEC mode

show ip ospf

This command displays information about the OSPF general configuration:

Syntax

`show ip ospf`

Comments? infodev@avaya.com

Command mode

Privileged EXEC mode

show ip ospf accept

This command displays information about the OSPF router acceptance parameter configuration:

Syntax

`show ip ospf accept`

Command mode

Privileged EXEC mode

show ip ospf area

This command displays information about the OSPF area configuration:

Syntax

`show ip ospf area`

Variable definitions

Use the following table to help you use the **`show ip ospf area`** command.

Variable	value
<cr>	Display ospf area information. <cr> is carriage return.
<*ipaddr*>	Display ospf area information with area ID. <ipaddr> is area ID.
area-range	Display ospf area range information
area-range <*ipaddr*>	Display ospf area range information with area ID. <ipaddr> is area ID.

Command mode

Privileged EXEC mode

show ip ospf ase

This command displays information about the OSPF external lsas configuration:

Syntax

`show ip ospf ase`

Variable definitions

Use the following table to help you use the **`show ip ospf ase`** command.

Variable	Value
<cr>	Display ospf external lsas information. <cr> is carriage return.
metric-type<*1-2*>	Display ospf external lsas metric-type information. <1-2> is metric type 1 or type 2.

Command mode

Privileged EXEC mode

show ip ospf authentication interface

This command displays information about the OSPF interface authentication configuration:

Syntax

`show ip ospf authentication interface`

Variable definitions

Use the following table to help you use the **`show ip ospf authentication interface`** command.

Variable	Value
<cr>	Display ospf authentication on interface. <cr> is carriage return.
vlan	Display ospf authentication on vlan interface.
vlan <*1-4094*>	Display ospf authentication on particular vlan interface. <1-4094> is the vlan ID.

Command mode

User EXEC mode

show ip ospf default-cost

This command displays information about the OSPF default-metric configuration:

Syntax

show ip ospf default-metric

Command mode

Privileged EXEC mode

show ip ospf host-route

This command displays information about the OSPF host-route configuration:

Syntax

show ip ospf host-route

Command mode

Privileged EXEC mode

show ip ospf ifstats

This command displays information about the OSPF interface statistics:

Syntax

show ip ospf ifstats [detail|mismatch|<ipaddr>]

Variable definitions

Use the following table to help you use the **show ip ospf ifstats [detail|mismatch|<ipaddr>]** command.

Variable	Value
detail	Shows detailed information of the statistics of ospf.
mismatch	Shows mismatch information.

Variable	Value
<ipaddr>	This is the interface ip address.

Command mode

Privileged EXEC mode

show ip ospf int-auth

This command displays information about the OSPF authentication configuration:

Syntax

show ip ospf int-auth

Command mode

Privileged EXEC mode

show ip ospf int-timers

This command displays information about the OSPF timers configuration:

Syntax

show ip ospf int-timers

Command mode

Privileged EXEC mode

show ip ospf interface

This command displays information about the OSPF interface configuration:

Syntax

show ip ospf interface

Variable definitions

Use the following table to help you use the **show ip ospf interfaces** command.

Variable	Value
<cr>	Display ospf interface information. <cr> is carriage return.
vlan	Display ospf vlan interface information.
vlan <*1-4094*>	Display ospf information on particular vlan interface. <1-4094> is the vlan ID.

Command mode

User EXEC mode

show ip ospf lsdb

This command displays information about the OSPF lsdb configuration:

Syntax

`show ip ospf lsdb`

Variable definitions

Use the following table to help you use the **`show ip ospf lsdb`** command.

Variable	Value
<cr>	Display ospf lsdb info information. <*cr*> is carriage return.
adv-rtr <*ipaddr*>	Display ospf lsdb information on particular advertisement router. <*ipaddr*> is router ID.
adv-rtr <*ipaddr*> detail	Display ospf detail lsdb information on particular advertisement router. <*ipaddr*> is router ID.
area <*ipaddr*>	Display ospf lsdb information on particular area. <*ipaddr*> is area ID.
detail	Display ospf detail lsdb information.
lsa-type <*0-7*>	Display particular type of ospf lsdb information. <*0-7*> is for typ1 to type 7.
lsid <ipaddr>	Display ospf lsdb infomation with a particular lsid. <*ipaddr*> is lsa ID.

Command mode

User EXEC mode

show ip ospf neighbours interface

This command displays information about OSPF neighbours:

Syntax

`show ip ospf neighbours interface`

Variable definitions

Use the following table to help you use the **`show ip ospf neighbours interface`** command.

Variable	Value
<cr>	Display all ospf neighbours. <cr> is carriage return.
vlan	Display all ospf neighbours on a vlan interface.
vlan <1-4094>	Display all ospf neighbours on a particular vlan interface. <*1-4094*> is the vlan ID.

Command mode

User EXEC mode

show ip ospf redistribute

This command displays information about the OSPF redistribute configuration.

Syntax

`show ip ospf redistribute`

Command mode

Privileged EXEC mode

show ip ospf stats

This command displays information about the OSPF statistics:

Syntax

`show ip ospf stats`

Command mode

Privileged EXEC mode

show ip ospf timer interface

This command displays information about OSPF interface timers:

Syntax

`show ip ospf timer interface`

Variable definitions

Use the following table to help you use the **`show ip ospf timer interface`** command.

Variable	Value
<cr>	Display ospf timers information on an interface. <cr> is carriage return.
vlan	Display ospf timers information on a vlan interface.
vlan <1-4094>	Display ospf timers information on a particular vlan interface. *<1-4094>* is the vlan ID.

Command mode

User EXEC mode

show ipv6 global

Use this command to view the IPv6 global parameters to verify the configuration.

syntax

`show ipv6 global`

Command mode

User EXEC mode

show ipv6 address ip

Use this command to view IPv6 interface addresses to learn the addresses.

syntax

`show ipv6 address ip [WORD <0-46>]`

Variable definitions

Use the data in the following table to help you use **`show ipv6 address ip`** command.

Variable	Value
WORD <0-46>	Specifies the IPv6 address and prefix length to assign to the management interface in the format IPv6address/prefix-length.

Command mode

User EXEC mode

show ipv6 route

Use this command to view IPv6 route information to learn the communication path between networks..

syntax

`show ipv6 route [static]`

Variable definitions

Use the data in the following table to help you use **`show ipv6 route`** command.

Variable	Value
[static]	Specifies a static route.

Command mode

User EXEC mode

show ipv6 neighbor

Use this command to view the IPv6 neighbor cache to discover information about neighbors in your network.

syntax

`show ipv6 neighbor [WORD <0-46>]`

Variable definitions

Use the data in the following table to help you use **`show ipv6 neighbor`** command.

Variable	Value
[WORD <0-46>]	Specifies the IPv6 address and prefix length to assign to the management interface in the format IPv6address/prefix-length.

Command mode

User EXEC mode

show ipv6 interface

Use this command to view the IPv6 interface to verify the configuration and to troubleshoot.

syntax

`show ipv6 interface [1-4094>]`

Variable definitions

Use the data in the following table to help you use **`show ipv6 interface`** command.

Variable	Value
[<1-4094>]	Specifies the interface index.

Command mode

User EXEC mode

show ipv6 nd-prefix [detail]

Use this command to view IPv6 neighbor discovery to learn about the source of an IP address or set of IP addresses.

syntax

`show nd-prefix [detail]`

Variable definitions

Use the data in the following table to help you use **`show ipv6 nd-prefix`** command.

Variable	Value
[detail]	Displays detailed neighbor determination information.

Command mode

User EXEC mode

show ip prefix-list

This command allows you to view prefix list information:

Syntax

`show ip prefix-list`

Command mode

Privileged EXEC mode

show ip rip

Use this command to display information about the RIP global configuration on the switch.

Syntax

`show ip rip`

Command mode

Privileged Exec mode

show ip rip interface

Use this command to display information about a specific RIP interface or all RIP interfaces on the switch.

Syntax

`show ip rip interface [vlan` *<1-4000>* **`]`**

Variable definitions

Use the following table to help you use the **`show ip rip interface vlan`** command.

Variable	Value
<1-4000>	This is the interface vlan id.

Command mode

Privileged mode

show ip routing

Use this command to display the status of IP routing on the switch.

Syntax

`show ip routing`

Command mode

Privileged Exec mode

show route-map

This command allows you to view a route policy.

Syntax

`show route-map [detail|vrf|vrfids]`

Variable definitions

Use the following table to help you use the **`show route-map`** command.

Variable	Value
detail	Displays the long format information of route-map.
vrf	Enter vrf to display route-map.
vrfids	Enter vrfids.

Command mode

Privileged EXEC mode

show ip route

This command allows you to view the route table.

Syntax

`show ip route [` *-s|alternative|count-summary|preference|static|vrf|vrfids|{A.B.C.D}*

Variable definitions

Use the following table to help you use the **`show ip route`** command.

Variable	Value
-s	Shows specific subnet {a.b.c.d/x|a.b.c.d/x.x.x.x|default}.
alternative	Shows alternative routes you wish to display.
count-summary	Displays route ip count summary.
preference	Shows route preference commands.
static	Shows statis route information.
vrf	Displays route for particular vrfs.
vrfids	Displays route for particular vrf ids.
{A.B.C.D}	IP address.

Command mode

Privileged EXEC mode

show ip tcp

Use this command to view the current TCP switch connections.

Syntax

`show ip tcp` <*connections*|*properties*|*statistics*>

Variable definitions

Use the following table too help you use the **`show ip tcp`** command.

variable	Value
connections	Displays ip tcp connections information commands.
properties	Displays ip tcp global properties commands.
statistics	Displays ip tcp global statistics commands.

Command mode

Privileged Exec mode

show lldp

This command displays the LLDP parameters for the neighbor system.

Syntax

`show lldp [interface|local-sys-data|mgmt-sys|neighbor|neighbor-mgmt-addr|neighbor-port-des|neighbor-sys-cap|neighbor-sys-des|neighbor-sys-name|pdu-tlv-size|rx-stats|stats|tx-stats|tx-tlv]`

Variable definitions

The following table describes variables that you enter in the **`show lldp`** command.

Variable	Value
interface	Displays LLDP port parameters.
local-sys-data	To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.
mgmt-sys	Displays the local management system data.

Variable	Value
neighbor	Displays the learned LLDP neighbors by port.
neighbor-mgmt-addr	Neighbor management address of LLDP
neighbor-port-des	Neighbor port description of LLDP.
neighbor-sys-cap	Neighbor system capability.
neighbor-sys-des	Neighbor system description.
neighbor-sys-name	Neighbor system name.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVS in an LLDP.
rx-stats	Displays the LLDP received statistics for ports on the local system.
stats	Displays the LLDP table statistics for the remote system.
tx-stats	Displays the LLDP transmit statistics for the ports on the local system.
tx-tlv	Displays which TLVs are transmitted from the local switch in the LLDP PDUs. To display the transmission status of the optional management TLVs for all the ports, include only the tx-tlv parameter in the compound.

The following table describes optional parameters that you enter after the **`show lldp`** command.

Variable	Value
`FastEthernet`	Fast Ethernet.
`GigabitEthernet`	Gigabit Ethernet.
`capabilities`	Displays system capabilities.
`chassis-id`	Displays the chassis id.
`detail`	Displays all TLVs.
`dot1`	Displays IEEE 802.1 organizationally specific TLVs.
`dot3`	Displays IEEE 802.3 organizationally specific TLVs.
`med`	Displays Media Endpoint Devices (MED) specific TLVs.
`port`	List of ports.

Variable	Value
sys-desc	Displays system description.
sys-name	Displays system name.

Command mode

Privileged Exec mode

show slpp

Use this command to display SLPP information.

Syntax

show slpp

Command mode

Privileged EXEC mode

show ports stats dhcp-relay

Use this command to display port statistics for dhcp-relay.

Syntax

show ports stats dhcp-relay broadcast [<ports>]

Command mode

Privileged EXEC mode

show vlan nlb-mode

Use this command to display the NLBS mode.

Syntax

show vlan nlb-mode

Command mode

Privileged EXEC mode

show snmp-server

Use this command to display the current SNMP settings.

Syntax

show snmp-server

Command mode

Privileged EXEC mode Global configuration mode Interface configuration mode

show eapol

This command displays the global settings updated to provide guest vlan and eap-mac-max information.

Syntax

show eapol

Variable definitions

The following table describes the variables that you use in the **show eapol** command.

Variable	Value
guest-vlan	Displays the EAPOL guest-vlan settings.
multihost	Displays the EAPOL multi-host settings.

Variable definitions

The following table describes the optional parameters that you use in the **show eapol** command.

Variable	Value
interface	Displays EAPOL per-port guest-vlan settings or the multihost port configuration.
non-eap-mac	Displays EAPOL multihost non-eap-mac port information.
status	Displays EAPOL multihost port status.

Command mode

Privileged Exec mode

Comments? infodev@avaya.com

show access-policy

Use this command to display the global access policy settings. If you specify a policy name, the settings for the policy are displayed.

Syntax

show access-policy *[by-mac|snmp-group|WORD<0-15>*

Variable definitions

Use the following table to help you use the **show access-policy** command.

Variable	Value
by-mac	Shows the access policy by mac information.
snmp-group	Shows the access-policy by snmp-group information.
WORD<0-15>	This is the access policy name with a length of 0 to 15 characters.

Command mode

Privileged EXEC mode

show nsna

Use this command to view information on the state of NSNA on the switch.

Syntax

show nsna

Command mode

Privileged EXEC mode

show nsna client

Use this command to view information on NSNA clients that are currently connected to the switch.

Syntax

`show nsna client [interface|mac-address]`

Variable definitions

Use the following table to help you use the **`show nsna client`** command.

Variable	Value
interface	Displays the nsna client port configuration.
mac-address	Displays the nsna client mac address.

show nsna nsnas

Use this command to view information related to the Avaya SNAS 4050 subnet.

Syntax

`show nsna nsnas <a.b.c.d/x.x.x.x>`

Variable definitions

Use the following table to help you use the **`show nsna nsnas`** command.

Variable	Value
<a.b.c.d/x.x.x.x>	This is the Avaya SNAS 4050 IP address and network mask.

Command mode

Privileged EXEC mode

show nsna interface

Use this command to view information related to the NSNA ports.

Syntax

`show nsna interface`

Command mode

Privileged EXEC mode:

show nsna phone-signature

Use this command to view configure NSNA phone signatures.

Syntax

`show nsna phone-signature`

Command mode

Privileged EXEC mode

show nsna vlan

Use this command to view information related to the NSNA VLANs.

Syntax

`show nsna vlan <1-4000>`

Variable definitions

Use the following table to help you use the **`show nsna vlan`** command.

Variable	Value
<1-4000>	This is the VLAN ID in the range 1-4000.

show radius

Use this command to display the global status of Remote Access Dial-in User Services (RADIUS) information.

Syntax

`show radius`

Command mode

Privileged EXEC mode

show radius-server

Use this command to display current Remote Access Dial-in User Services (RADIUS) server configurations and statistics.

Syntax

`show radius-server`

Variable definitions

Use the following table to help you use the **`show radius-server`** command.

Variable	Value
accounting-stat	Shows the radius accounting statistics.
authentication-stat	Shows the radius authentication statistics.
statistics	Shows the radius server statistics.

Command mode

Privileged EXEC mode

show sys log host

Use this command to display system log information for a specified host.

Syntax

`show sys log host` <*1-10*>

Variable definitions

Use the following table to help you use the **`sys log host`** command.

Variable	Value
<*1-10*>	Specifies the host ID number.

Command mode

Privileged EXEC mode

show boot config

Use this command to display the current configuration of the Boot Monitor and the Boot Monitor CLI.

Syntax

`show boot config`

Variable definitions

Use the following table to help you use the **`show boot config`** command.

Variable	Value
bootp	
choice	Displays the current boot configuration choices.
cli	Displays the current Boot Monitor CLI configuration.
config	Displays the current Boot Monitor configuration.
flags	Displays the current flag settings for the switch.
host	Displays the current host configuration.
info	Displays information about the switch boot image.
master	Displays the slot where the Master CPU resides and the settings for the delay and multicast commands.
net	Displays the current configuration of the CPU network ports.
sio	Displays the current configuration of the CPU serial ports.
tz	Displays the switch's current time zone settings.

Command mode

Privileged EXEC mode

show boot config choice

Use this command to display the current boot configuration choices.

Syntax

show boot config choice

Command mode

Privilege EXEC mode

show boot config cli

Use this command to display the current configuration of the Boot Monitor CLI.

Syntax

show boot config cli

Command mode

Privilege EXEC mode

show boot config config

Use this command to display the current configuration of the Boot Monitor.

Syntax

show boot config config

Command mode

Privileged EXEC mode

show boot config flags

Use this command to display the current flag settings for the switch.

Syntax

show boot config flags

Command mode

Privileged EXEC mode

show boot config host

Use this command to display the current configuration of the host.

Syntax

show boot config host

Command mode

Privileged EXEC mode

show boot config info

Use this command to display information about the switch boot image.

Syntax

show boot config info

Command mode

Privileged EXEC mode

show boot config master

Use this command to display the slot where the Master CPU resides and to display the settings for the **boot config delay** and **boot config multicast** commands.

Syntax

show boot config master

Command mode

Privilege EXEC mode

show boot config net

Use this command to display the current configuration of the CPU network ports.

Syntax

show boot config net

Command mode

Privilege EXEC mode

show boot config sio

Use this command to display the current configuration of the CPU serial ports.

Syntax

show boot config sio

Command mode

Privilege EXEC mode

show boot config tz

Use this command to display the current time zone settings on the switch.

Syntax

show boot config tz

Command mode

Privilege EXEC mode

show autotopology

Use this command to display the topology table. The topology table shows the information that is sent to Optivity network management software for creating network displays.

Syntax

show autotopology nmm-table

Command mode

Privilege EXEC mode

show basic config

Use this command to display information for the auto-recover-delay.

Syntax

show basic config

Command mode

Privilege EXEC mode

show interfaces GigabitEthernet interface

This command displays the MTU values for all ports on the chassis.

Syntax

show interfaces GigabitEthernet interface [portlist]

Command mode

User Exec mode

show link-flap-detect

Use this command to display the link-flap-detect settings.

Syntax

show link-flap-detect

Command mode

Privilege EXEC mode

show logging config

Use this command to display the level of information being entered in the log. The levels range from information (INFO), where all messages are entered, to FATAL, where only fatal errors are recorded. The manufacturing (MFG) level is for manufacturing purposes only and not available for customer use.

Syntax

show logging config

Command mode

Privilege EXEC mode

show logging file

Use this command to display the selected log file.

Syntax

show logging file [category] [CPU] [name-of-file] [save-to-file] [severity] [tail]

Variable definitions

Use the following table to help you use the **show logging file** command.

Variable	Value
[category <*string*>]	Specifies the category of log file information to display for the **show logging** command. The range of characters is 0 to 100.
[CPU <*integer*>]	Specifies the CPU number for which to display log file information.The range of values is 0 to 25.
[name-of-file <*string*>]	Specifies the file for which to display log information. The range of characters is 1 to 99.
[save-to-file <*string*>]	Specifies the file to save log file information to. The range of characters is 1 to 99.
[severity <*string*>]	Specifies the severity level for which to display log information. The range of characters is 0 to 25.
[tail]	Specifies displaying the log file in reverse order, with the most recent information first.

Command mode

Privileged EXEC mode

show log filter

Use this command to display the log filter configuration.

Syntax

show log filter

Command mode

Privilege EXEC mode

show running-config

Use this command to display information about the current switch configuration.

Syntax

show running-config

Command mode

Privilege EXEC mode

show slot

Use this command to display the administrative status of the module.

Syntax

show slot <*slot-number*>

Variable definitions

Use the following table to help you use the **show slot** command:

Variable	Value
<*slot-number*>	specifies the slot number in the chassis. The range of values is 1 to 10.

	Important: Slots are numbered from top to bottom in Ethernet Routing Switch 8300 switches

Command mode

Privilege EXEC mode

show sys hash-calc mltindex ip dest-mac dest-ip src-mac src-ip src-port mlt

Use this command to calculate unicast IP traffic distribution.

Syntax

show sys hash-calc mltindex ip dest-mac <*value*>**dest-ip** <*value*>**src-mac**<*value*>**src-ip**<*value*>**src-port**,*value*>**mlt**<*value*>

Variable definitions

Use the following table to help you use the **show sys hash-calc mltindex ip dest-mac dest-ip src-mac src-ip src-port mlt** command.

Variable	Value
dest-mac <*value*>	Specifies the destination MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00}.
dest-ip<*value*>	Specifies the destination IP address {a.b.c.d}
src-mac<*value*>	Specifies the source MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00}.
src-ip<*value*>	Specifies the source IPaddress {a.b.c.d}.
src-port <*value*>	Specifies the ingress port in the format {slot/port}.
mlt<*value*>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Command mode

Global configuration mode

Comments? infodev@avaya.com

show sys hash-calc mltindex non-ip dest-mac src-mac src-port mlt

Use this command to calculate unicast non-IP distribution.

Syntax

show sys hash-calc mltindex non-ip dest_mac <*value*>**src-mac**<*value*>**src-port**,*value*>**mlt**<*value*>

Variable definitions

Use the following table to help you use the **show sys hash-calc mltindex non-ip dest-mac src-mac src-port mlt** command.

Variable	Value
dest-mac <*value*>	Specifies the destination MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00:0x00}.
src-mac<*value*>	Specifies the source MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00:0x00}.
src-port <*value*>	Specifies the ingress port in the format {slot/port}.
mlt<*value*>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Commande mode

Global configuration mode

show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt

Use this command to calculate multicast traffic distribution.

Syntax

show sys hash-calc mltindex ip-mcast source <*value*>**group**<*value*>**vlan-id**<*value*>**src-port**,*value*>**mlt**<*value*>

Variable definitions

Use the following table to help you use the **show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt** command.

Variable	Value
source <*value*>	Specifies the multicast source address {a.b.c.d}.
group<*value*>	Specifies the multicast source address {a.b.c.d}.
vlan-id <value>	Specifies the VLAN ID. Value is an integer from 1 to 4000. The egress VLAN ID is used for IP-Mcast hash.
src-port <*value*>	Specifies the ingress port in the format {slot/port}.
mlt<*value*>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Command mode

Global configuration mode

show sys hash-calc mltindex non-ip-mcast dest-mac vlan-id src-port mlt

Use this command to calculate non-IP multicast traffic distribution.

Syntax

show sys hash-calc mltindex non-ip-mcast dest-mac<*value*>**vlan-id**<*value*>**src-port**,*value*>**mlt**<*value*>

Variable definitions

Use the following table to help you use the **show sys hash-calc mltindex non-ip-mcast dest-mac vlan-id src-port mlt** command:

Variable	Value
dest-mac< *value*>	Specifies the destination mac address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00}.
vlan-id<*value*>	Specifies the VLAN ID. Value is an integer from 1 to 4000. The egress VLAN ID is used for IP-Mcast hash.

Comments? infodev@avaya.com

Variable	Value
src-port <*value*>	Specifies the ingress port in the format {slot/port}.
mlt<*value*>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Command mode

Global configuration mode

show sys-info

Use this command to display the system status and technical information about the configuration of switch hardware components.

This command displays general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, and topology status.

Syntax

`show sys-info` *[card] [asic] [mda]*

Variable definitions

Use the following table to help you use the **`show sys-info`** command.

Variable	Value
[card]	Displays information about all the installed modules.
[asic]	Displays information about the ASICS installed on each module.
[mda]	Displays information about installed MDAs.

Command mode

Privileged EXEC mode

show sys perf

Use this command to display system performance information, such as CPU and switch fabric utilization and NVRAM size and use. The information is updated once per second, so it is no more than one second from real time.

Syntax

`show sys perf`

Command mode

Privileged EXEC mode

show sys sw

Use this command to display the version of software running on the switch, the last update of the software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags.

Syntax

`show sys sw`

Command mode

Privileged EXEC mode

show ip vrf

Use this command to ensure that the vrf instance is configured correctly.

Syntax

`show ip vrf <WORD 0-32>`

<*WORD 0-32*> is the name of the VRF instance with a string length of 0 to 32.

Variable definitions

Use the data in the following table to help you use the **`show ip vrf <WORD 0-32>`** command.

Variable	Value
<cr>	Displays information about all VRF instances.
max-routes [vrfids<WORD 0-127>][WORD <0-32>]	Displays the maximum number of routes for the specified VRFs. • vrfids <WORD 0-127> specifies a list of VRFs by VRF IDs. • <WORD 0-32> specifies a VRF name.
vrfids <WORD 0-127>	Specifies a list of VRFs by VRFIDs

Comments? infodev@avaya.com

Command mode

Global configuration mode

Comments? infodev@avaya.com

Chapter 20: Customer Service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Comments? infodev@avaya.com

Index

A

accessing 207
  loopback interface mode 207
activity check interval 382
ARP table, clearing specified entries 37
auto-negotiate command (Run-Time CLI) 331
automatic trace, configuring using the ACLI 57

B

backup CPU, activating 54
Boot Monitor 543
  configuration, displaying 543

C

choice commands 64–66
  Run-Time CLI 64–66
config ip route-policy commands 251
configuration 543
  displaying 543
    Boot Monitor 543
configuration file 70
  debugging 70
counters, resetting 54
CPU 543
  master 543

D

daylight saving time, setting 70, 72
daylight-saving-time flag 70, 72
debug-config flag 70

E

EAPoL 140
  configuring ports 140

F

factorydefaults flag 70
flag settings, displaying 543
FTP, enabling 70, 72
ftpd flag 70

I

IGMP ACLI commands 534
  show ip route 534
IP route-policy commands 251
  configure 251

L

logging flag 70
loopback interface mode, accessing 207

M

master CPU 543
  displaying location 543

P

PIM-SM 382
  activity check interval 382

R

reboot flag 70
RIP commands 532
  show 532

S

show ip rip command 532
show ip rip interface command 533

T

table, flushing 37
Telnet sessions 37
  ending 37
telnetd flag 70, 72
tftpd flag 70, 72
timer, watchdog 70

V

viewing the route table in the ACLI 534

W

watchdog timer 70
wdt flag 70